LINKSYS®

A Division of Cisco Systems, Inc.



2,4 GHz 802.11g

Wireless-G

ADSL Home Gateway

User Guide





Model No. **WAG354G (EU)**

Copyright and Trademarks

How to Use this Guide

Your Guide to the Wireless-G ADSL Home Gateway has been designed to make understanding networking with the Gateway easier than ever. Look for the following items when reading this User Guide:



This checkmark means there is a Note of interest and is something you should pay special attention to while using the Gateway.



This exclamation point means there is a Caution or Warning and is something that could damage your property or the Gateway.



This question mark provides you with a reminder about something you might need to do while using the Gateway.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: *definition.*

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

WAG354G-EU-UG-50429C JL

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G ADSL Home Gateway. This Gateway will provide your computers with a high-speed Internet connection as well as resources, including files and printers. Since the Gateway is wireless, Internet access can be shared over the wired network as well as the wireless broadcast at up to 11Mbps for Wireless-B or up to 54Mbps for Wireless-G.

How does the Gateway do all of this? By connecting the Internet, as well as your computers and peripherals, to the Gateway, then the Gateway can direct and control communications for your network.

To protect your data and privacy, the Gateway features an advanced firewall to keep out Internet intruders. Wireless transmissions can be protected by powerful data encryption. In addition, you can safeguard your family with parental control features such as Internet access restrictions and keyword blocking. You can configure the Gateway's settings through the easy-to-use, browser-based utility.

But what does all of this mean?

Networks are useful tools for sharing Internet access and computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks not only are useful in homes and offices, but also can be fun.

PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called "wired". PCs equipped with wireless cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wireless Local Area Network. Since the Gateway has wireless capabilities, it can bridge your wired and wireless networks, letting them communicate with each other.

With your networks all connected, wired, wireless, and the Internet, you can now share files and Internet access—and even play games. All the while, the Wireless-G ADSL Home Gateway protects your networks from unauthorized and unwelcome users.

Linksys recommends using the Setup CD-ROM for first-time installation of the Gateway. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then use the instructions in this Guide to help you connect the Gateway, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Wireless-G ADSL Home Gateway.

wpa *(wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.*

spi *(stateful packet inspection)* ***firewall****: a technology that inspects incoming packets of information before allowing them to enter the network.*

firewall*: Security measures that protect the resources of a local network from intruders.*

nat *(network address translation): NAT technology translates IP addresses of a local area network to a different IP address for the Internet.*

network*: a series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users*

lan *(local area network): The computers and networking products that make up the network in your home or office.*

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-G ADSL Home Gateway.

- Chapter 1: Introduction
  This chapter describes applications of the Wireless-G ADSL Home Gateway and this User Guide.

- Chapter 2: Planning Your Network
  This chapter describes the basics of networking.

- Chapter 3: Getting to Know the Wireless-G ADSL Home Gateway
  This chapter describes the physical features of the Gateway.

- Chapter 4: Connecting the Wireless-G ADSL Home Gateway
  This chapter instructs you on how to connect the Gateway to your network.

- Chapter 5: Configuring the Wireless-G ADSL Home Gateway
  This chapter explains how to use the Web-based Utility to configure the settings on the Gateway.

- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G ADSL Home Gateway.

- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.

- Appendix C: Finding the MAC Address and IP Address for your Ethernet Adapter.
  This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Gateway.

- Appendix D: Upgrading Firmware
  This appendix instructs you on how to upgrade the firmware on the Gateway if you should need to do so.

- Appendix E: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.

- Appendix F: Specifications
  This appendix provides the technical specifications for the Gateway.

- Appendix G: Warranty Information
  This appendix supplies the warranty information for the Gateway.

- Appendix H: Regulatory Information
  This appendix supplies the regulatory information regarding the Gateway.

- Appendix I: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Network

The Gateway's Functions

A Gateway is a network device that connects two networks together.

In this instance, the Gateway connects your Local Area Network (LAN), or the group of computers in your home or office, to the Internet. The Gateway processes and regulates the data that travels between these two networks.

The Gateway's NAT feature protects your network of computers so users on the public, Internet side cannot "see" your computers. This is how your network remains private. The Gateway protects your network by inspecting every packet coming in through the Internet port before delivery to the appropriate computer on your network. The Gateway inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate computer on the LAN side.

Remember that the Gateway's ports connect to two sides. The LAN ports connect to the LAN, and the ADSL port connects to the Internet. The LAN ports transmit data at 10/100Mbps.



Figure 2-1: Network

IP Addresses

What's an IP Address?

IP stands for Internet Protocol. Every device on an IP-based network, including computers, print servers, and Gateways, requires an IP address to identify its "location," or address, on the network. This applies to both the Internet and LAN connections. There are two ways of assigning an IP address to your network devices. You can assign static IP addresses or use the Gateway to assign IP addresses dynamically.

ip *(internet protocol): a protocol used to send data over a network*

Static IP Addresses

A static IP address is a fixed IP address that you assign manually to a computer or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses must be unique and are commonly used with network devices such as server computers or print servers.



NOTE: Since the Gateway is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this User Guide, you'll see references to the "Internet IP address" and the "LAN IP address."

Since the Gateway uses NAT technology, the only IP address that can be seen from the Internet for your network is the Gateway's Internet IP address. However, even this Internet IP address can be blocked, so that the Gateway and network seem invisible to the Internet—see the Block WAN Requests description under Security in "Chapter 5: Configuring the Wireless-G ADSL Home Gateway."

Since you use the Gateway to share your DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the Gateway. You can get that information from your ISP.

Dynamic IP Addresses

A dynamic IP address is automatically assigned to a device on the network, such as computers and print servers. These IP addresses are called "dynamic" because they are only temporarily assigned to the computer or device. After a certain time period, they expire and may change. If a computer logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will automatically assign it a new dynamic IP address.

DHCP (Dynamic Host Configuration Protocol) Servers

Computers and other network devices using dynamic IP addressing are assigned a new IP address by a DHCP server. The computer or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

A DHCP server can either be a designated computer on the network or another network device, such as the Gateway. By default, the Gateway's DHCP Server function is enabled.

If you already have a DHCP server running on your network, you must disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Gateway, see the DHCP section in "Chapter 5: Configuring the Wireless-G ADSL Home Gateway."

Chapter 3: Getting to Know the Wireless-G ADSL Home Gateway

Ports and Reset Button on Side Panel

The Gateway's ports and Reset button are located on a side panel.

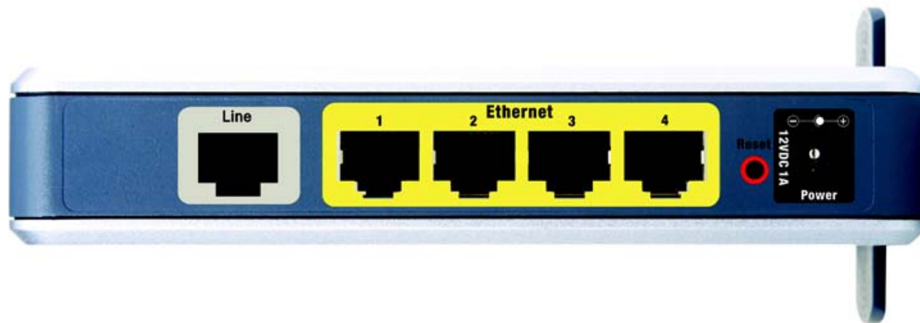


Figure 3-1: Ports and Reset Button on Side Panel

Line The **Line** port connects to the ADSL line.

Ethernet (1-4) The **Ethernet** ports connect to your computers and other network devices.

Reset Button There are two ways to reset the Gateway's factory defaults. Either press the **Reset Button**, for approximately ten seconds, or restore the defaults from the *Factory Defaults* screen of the Administration tab in the Gateway's Web-based Utility.

Power The **Power** port is where you will connect the power adapter.



IMPORTANT: Resetting the Gateway to factory defaults will erase all of your settings (including Internet connection, wireless, and other settings) and replace them with the factory defaults. Do not reset the Gateway if you want to retain these settings.

LEDs on Side Panel

The Gateway's LEDs, which indicate network activity, are located on the other side panel.



Figure 3-2: LEDs on Side Panel

POWER Green. The **POWER** LED lights up when the Gateway is powered on.

WIRELESS Green. The **WIRELESS** LED lights up whenever there is a successful wireless connection. If the LED is flashing, the Gateway is actively sending or receiving data to or from one of the devices on the network.

ETHERNET (1-4) Green. The **ETHERNET** LED serves two purposes. If the LED is continuously lit, the Gateway is successfully connected to a device through the LAN port. If the LED is flashing, it is an indication of any network activity.

DSL Green. The **DSL** LED lights up whenever there is a successful DSL connection. The LED blinks while the Gateway is establishing the ADSL connection.

INTERNET Green. The **INTERNET** LED lights up green when an Internet connection to the Internet Service Provider (ISP) is established. The **INTERNET** LED lights up red when the connection to the ISP fails.

The Top Panel

The Gateway comes with a built-in antenna; however, you can attach an optional antenna. (Note: This antenna is currently not available in Europe.) The Linksys 5dBi High Gain Antenna for SMA Connectors (model number: HGA5S) is available for increased range. The Gateway's SMA port for the optional antenna is located on the top panel. To access the SMA port, push the tab. To attach the antenna, insert the base of the antenna into the SMA port and tighten it clockwise by hand.



Figure 3-3: Top Panel

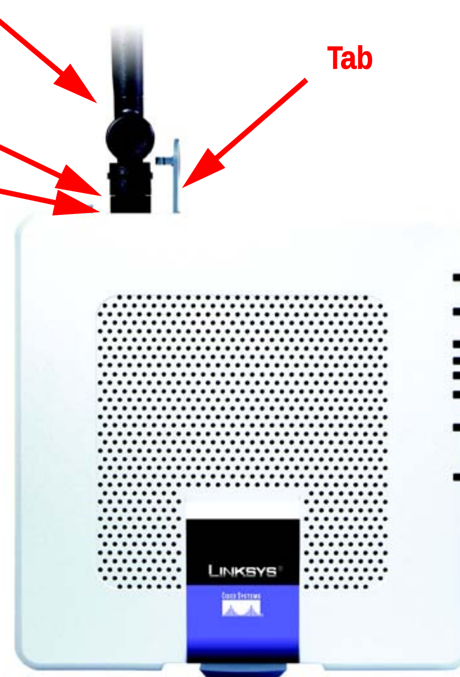


Figure 3-4: Top Panel with Optional Antenna

The Bottom Panel

The Gateway has a built-in stand available. If you place the Gateway flat on a surface, then you can leave the stand in the closed position. However, if you want the Gateway to be upright, swivel the stand clockwise 90º and position the Gateway accordingly.



Figure 3-5: Bottom Panel with Stand in Closed Position



Figure 3-6: Gateway Using Stand

Chapter 4: Connecting the Wireless-G ADSL Home Gateway

Overview

The installation technician from your ISP should have left the setup information for the modem with you after installing your broadband connection. If not, you can call your ISP to request that data.

After you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Gateway.

If you want to use a computer with an Ethernet adapter to configure the Gateway, continue to “Wired Connection to a Computer.” If you want to use a computer with a wireless adapter to configure the Gateway, continue to “Wireless Connection to a Computer.”

Wired Connection to a Computer

1. Make sure that all of your network's hardware is powered off, including the Gateway and all computers.

2. Connect a phone cable from the Line port on the Gateway's side panel to the wall jack of the ADSL line. A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.



Figure 4-1: Connect the ADSL Line



NOTE: A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.



IMPORTANT: For countries that have phone jacks with RJ-11 connectors, make sure to only place the microfilters between the phone and the wall jack and **not** between the Gateway and the wall jack or your ADSL will not connect.

For countries that do **not** have phone jacks with RJ-11 connectors (e.g. France, Sweden, Switzerland, United Kingdom, etc.), except for ISDN users, the microfilter has to be used between the Gateway and the wall jack, because the microfilter will have the RJ-11 connector.

Annex B users (E1 and DE versions of the Gateway) must use the included special cable to connect the Gateway to the wall jack (RJ-45 to RJ-12). If you require splitters or special jacks, please contact your service provider.

3. Connect one end of an Ethernet network cable to one of the Ethernet ports (labeled 1-4) on the back of the Gateway, and the other end to an Ethernet port on a computer.

   Repeat this step to connect more computers, a switch, or other network devices to the Gateway.



Figure 4-2: Connect a PC

4. Connect the power adapter to the Gateway's Power port, and then plug the power adapter into a power outlet.



NOTE: You should always plug the Gateway's power adapter into a power strip with surge protection.

   The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, and then it will be solidly lit when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."



Figure 4-3: Connect the Power

5. Power on one of your computers that is connected to the Gateway.

Go to "Chapter 5: Configuring the Wireless-G ADSL Home Gateway."

Wireless Connection to a Computer

If you want to use a wireless connection to access the Gateway, follow these instructions:

1. Make sure that all of your network's hardware is powered off, including the Gateway and all computers.

2. Connect a phone cable from the Line port on the Gateway's back panel to the wall jack of the ADSL line. A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.



NOTE: A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.



IMPORTANT: For countries that have phone jacks with RJ-11 connectors, make sure you only place the microfilters between the phone and the wall jack and **not** between the Gateway and the wall jack or your ADSL will not connect.

For countries that do **not** have phone jacks with RJ-11 connectors (e.g. France, Sweden, Switzerland, United Kingdom, etc.), except for ISDN users, the microfilter has to be used between the Gateway and the wall jack, because the microfilter will have the RJ-11 connector.

Annex B users (E1 and DE versions of the Gateway) must use the included special cable to connect the Gateway to the wall jack (RJ-45 to RJ-12). If you require splitters or special jacks, please contact your service provider.

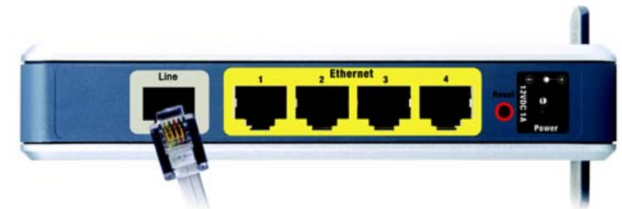


Figure 4-4: Connect the ADSL Line

3. Connect the power adapter to the Power port, and then plug the power adapter into a power outlet.

   The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, and then it will be solidly lit when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."

4. Power on one of the computers on your wireless network(s).

5. For initial access to the Gateway through a wireless connection, make sure the computer's wireless adapter has its SSID set to **linksys** (the Gateway's default setting), and its wireless security is disabled. After you have accessed the Gateway, you can change the Gateway and this computer's adapter settings to match your usual network settings.

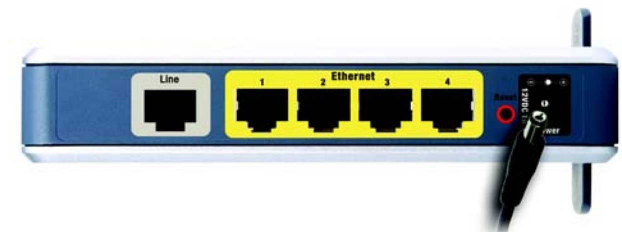


Figure 4-5: Connect the Power

Go to "Chapter 5: Configuring the Wireless-G ADSL Home Gateway."



NOTE: You should always change the SSID from its default, **linksys**, and enable wireless security.

Chapter 5: Configuring the Wireless-G ADSL Home Gateway

Overview

Follow the steps in this chapter and use the Gateway's web-based utility to configure the Gateway. This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Gateway. For a basic network setup, most users only have to use the following screens of the Utility:

- Basic Setup. On the Basic Setup screen, enter the settings provided by your ISP.
- Management. Click the **Administration** tab and then the **Management** tab. The Gateway's default username and password is admin. To secure the Gateway, change the Password from its default.

There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

Setup

- Basic Setup. Enter the Internet connection and network settings on this screen.
- DDNS. To enable the Gateway's Dynamic Domain Name System (DDNS) feature, complete the fields on this screen.
- Advanced Routing. On this screen, you can alter NAT and routing configurations.

Wireless

- Basic Wireless Settings. You can choose your wireless network settings on this screen.
- Wireless Security. Configure your wireless security settings on this screen.
- Wireless Access. This screen lets you control access to your wireless network.
- Advanced Wireless Settings. On this screen you can access the advanced wireless network settings.



HAVE YOU: Enabled TCP/IP on your computers? Computers communicate over the network with this protocol. Refer to Windows Help for more information on TCP/IP.



NOTE: For added security, you should change the password through the Administration tab.

Security

On this screen you can disable or enable the firewall, set up filters, block WAN requests, and enable or disable Virtual Private Networks (VPN) PassThrough.

vpn *(virtual private network): a security measure to protect data as it leaves one network and goes to another over the Internet.*

Access Restrictions

- Internet Access. This screen allows you to control the Internet usage and traffic on your local network.

Applications & Gaming

- Single Port Forwarding. Use this screen to set up common services or applications that require forwarding on a single port.
- Port Range Forwarding. To set up public services or other specialized Internet applications that require forwarding on a range of ports, use this screen.
- Port Triggering. To set up triggered ranges and forwarded ranges for Internet applications, click this tab.
- DMZ. To allow one local computer to be exposed to the Internet for use of special-purpose services, use this screen.
- QoS. Use Quality of Service (QoS) to assign different priority levels to different types of data transmissions.

Administration

- Management. On this screen, alter Gateway access, Simple Network Management Protocol (SNMP), Universal Plug and Play (UPnP), IGMP-Proxy (IGMP stands for Internet Group Multicast Protocol), and wireless management settings.
- Reporting. If you want to view or save activity logs, click this tab.
- Diagnostics. Use this screen to run a Ping test.
- Backup&Restore. On this screen, you can back up or restore the Gateway’s configuration.
- Factory Defaults. If you want to restore the Gateway’s factory default settings, use this screen.
- Firmware Upgrade. Click this tab if you want to upgrade the Gateway’s firmware.
- Reboot. If you need to do a hard or soft reboot of the Gateway, use this screen.

Status

- Gateway. This screen provides status information about the Gateway.
- Local Network. This provides status information about the local network.
- Wireless. This screen provides status information about the wireless network.
- DSL Connection. This screen provides status information about the DSL connection.



Figure 5-1: Login Screen

How to Access the Web-based Utility

To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Gateway's default IP address, **192.168.1.1**, in the *Address* field. Then press **Enter**.

A login screen will appear (Windows XP users will see a similar screen). Enter **admin** (the default user name) in the *User Name* field, and enter **admin** (the default password) in the *Password* field. Then click the **OK** button.

The Setup Tab

The Basic Setup Tab

The first screen that appears is the Basic Setup tab. This tab allows you to change the Gateway's general settings. Change these settings as described here and click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to cancel your changes.

Internet Setup

- Internet Connection Type. The Gateway supports five Encapsulation methods: RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA, and Bridged Mode Only. Select the appropriate type of encapsulation from the drop-down menu. Each *Basic Setup* screen and available features will differ depending on what type of encapsulation you select.
- VC Settings. You will configure your Virtual Circuit (VC) settings in this section.
  - Multiplexing: Select **LLC** or **VC**, depending on your ISP.
  - QoS Type: Select from the drop-down menu: **CBR** (Continuous Bit Rate) to specify fixed bandwidth for voice or data traffic; **UBR** (Unspecific Bit Rate) for application that are none-time sensitive, such as e-mail; or **VBR** (Variable Bite Rate) for Bursty traffic and bandwidth-sharing with other applications.

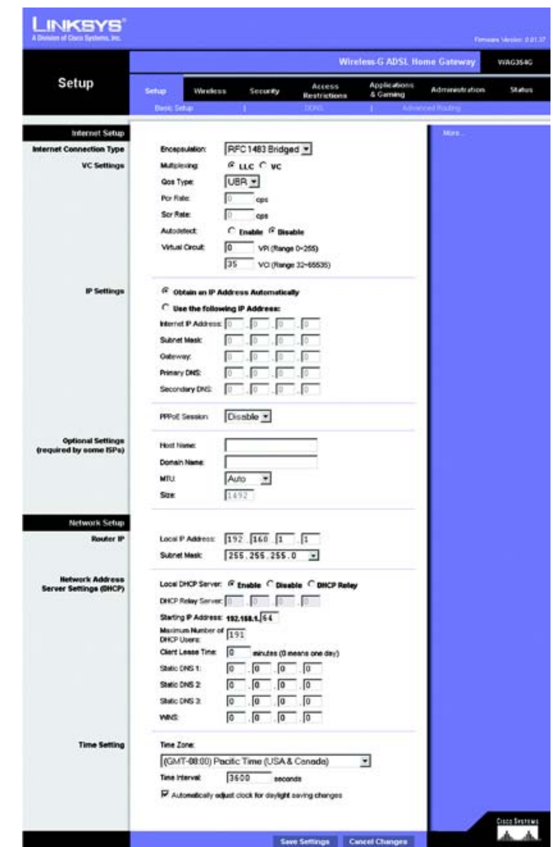


Figure 5-2: Basic Setup

- Pcr Rate: For the Peak Cell Rate, divide the DSL line rate by 424 to get the maximum rate the sender can send cells. Enter the rate in the field (if required by your service provider).
- Scr Rate: The Sustain Cell Rate sets the average cell rate that can be transmitted. The SCR value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).
- Autodetect: Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.
- Virtual Circuit: These fields consist of two items: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields.

- IP Settings. Follow the instructions in the section for your type of encapsulation.

RFC 1483 Bridged

Dynamic IP

IP Settings. Select **Obtain an IP Address Automatically** if your ISP says you are connecting through a dynamic IP address.

Figure 5-3: RFC 1483 Bridged - Dynamic IP

Static IP

If you are required to use a permanent (static) IP address to connect to the Internet, then select **Use the following IP Address**.

- Internet IP Address. This is the Gateway's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Gateway's Subnet Mask. Your ISP will provide you with the Subnet Mask.
- Gateway. Your ISP will provide you with the default Gateway Address, which is the ISP server's IP address.
- Primary DNS (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Figure 5-4: RFC 1483 Bridged - Static IP

RFC 1483 Routed

If you are required to use RFC 1483 Routed, then select **RFC 1483 Routed**.

- Internet IP Address. This is the Gateway's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Gateway's Subnet Mask. Your ISP will provide you with the Subnet Mask.
- Gateway. Your ISP will provide you with the default Gateway Address, which is the ISP server's IP address.
- Primary DNS (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Figure 5-5: RFC 1483 Routed

RFC 2516 PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE.

- Service Name. Enter the name of your PPPoE service in this field.
- User Name and Password. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Gateway to disconnect the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, click the **Connect on Demand** radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive: Redial Period. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, click the **Keep Alive** radio button. In the *Redial Period* field, specify how often you want the Gateway to check the Internet connection. The default Redial Period is **20** seconds.

Figure 5-6: RFC 2516 PPPoE

RFC 2364 PPPoA

Some DSL-based ISPs use PPPoA (Point-to-Point Protocol over ATM) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoA. If they do, you will have to enable PPPoA.

- User Name and Password. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Gateway to disconnect the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, click the **Connect on Demand** radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive: Redial Period. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, click the **Keep Alive** radio button. In the *Redial Period* field, specify how often you want the Gateway to check the Internet connection. The default Redial Period is **20** seconds.

Figure 5-7: RFC 2364 PPPoA

Bridged Mode Only

If you are using your Gateway as a bridge, which makes the Gateway act like a stand-alone modem, select **Bridged Mode Only**. All NAT and routing settings are disabled in this mode.

Figure 5-8: Bridged Mode Only

Optional Settings (required by some ISPs)

- Host Name and Domain Name. These fields allow you to supply a host and domain name for the Gateway. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, you can leave these fields blank.
- MTU and Size. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select **Manual** and enter the value desired in the *Size* field. It is recommended that you leave this value in the 1200 to 1500 range. By default, MTU is configured automatically.

Network Setup

- Router IP. The values for the Gateway's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work.

- Local IP Address. The default value is **192.168.1.1**.
- Subnet Mask. The default value is **255.255.255.0**.

- Network Address Server Settings (DHCP). Configure the Gateway's Dynamic Host Configuration Protocol (DHCP) settings in this section.
  - Local DHCP Server. A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each computer on your network for you. Unless you already have one, it is highly recommended that you leave the Gateway enabled as a DHCP server. You can also use the Gateway in DHCP Relay mode.
  - DHCP Relay Server. If you enable the DHCP Relay mode for the *Local DHCP Server* setting, enter the IP address for the DHCP server in the fields provided.
  - Starting IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1. 2 or greater, because the default IP address for the Gateway is 192.168.1.1.
  - Maximum Number of DHCP Users. Enter the maximum number of users/clients that can obtain an IP address. The number will vary depending on the starting IP address entered.
  - Client Lease Time. The Client Lease Time is the amount of time a computer will be allowed connection to the Gateway with its current dynamic IP address. Enter the amount of time, in minutes, that the computer will be "leased" this dynamic IP address.
  - Static DNS 1-3. The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. You can enter up to three DNS Server IP Addresses here. The Gateway will use these for quicker access to functioning DNS servers.
  - WINS. The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank.
  - Time Setting. Select the appropriate time zone for the Gateway's location. If desired, check the **Automatically adjust clock for daylight saving changes** checkbox.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Figure 5-9: Optional Settings

The DDNS Tab

The Gateway offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Gateway.

Before you can use this feature, you need to sign up for DDNS service at DynDNS.org or TZO.com.

DDNS

DDNS Service. If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** from the drop-down menu. If your DDNS service is provided by TZO.com, then select **TZO.com** from the drop-down menu.To disable DDNS Service, select **Disabled**.



Figure 5-10: DynDNS.org

DynDNS.org

- User Name, Password, and Host Name. Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.
- Internet IP Address. The Gateway's current Internet IP Address is displayed here. Because it is dynamic, it will change.
- Status. The status of the DDNS service connection is displayed here.

TZO.com

- E-mail Address, Password, and Domain Name. Enter the E-mail Address, Password, and Domain Name of the account you set up with TZO.
- Internet IP Address. The Gateway's current Internet IP Address is displayed here. Because it is dynamic, this will change.
- Status. The status of the DDNS service connection is displayed here.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Figure 5-11: TZO.com

The Advanced Routing Tab

The *Advanced Routing* screen allows you to configure the NAT, dynamic routing, and static routing settings.

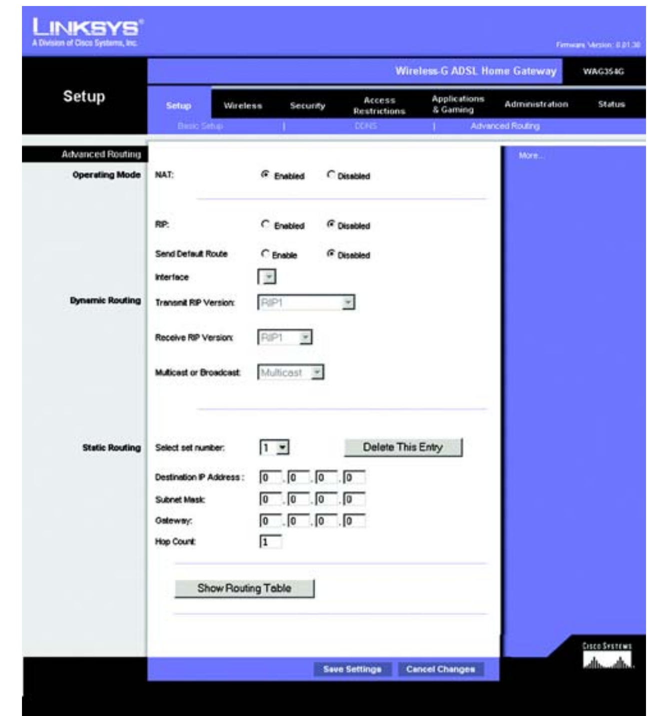


Figure 5-12: Advanced Routing

Advanced Routing

- Operating Mode. In this section, you will configure the Gateway's general routing settings.
  - NAT. NAT is a security feature that is enabled by default. It enables the Gateway to translate IP addresses of your local area network to a different IP address for the Internet. To disable NAT, click the **Disabled** radio button.
  - RIP. If you have multiple routers, you may want to use the Routing Information Protocol (RIP) so the routers can exchange routing information with each other. To use RIP, select the **Enabled** radio button. Otherwise, keep the default, **Disabled**.
  - Send Default Route. To use RIP version 1 for routing, select the **Enabled** radio button. Otherwise, keep the default, **Disabled**.
  - Interface. This setting is available when you have configured a static route and you need to choose an interface for that route. Select the interface that the Gateway will be using: **LAN/Wireless** or **Internet**.
- Dynamic Routing. With Dynamic Routing you can enable the Gateway to automatically adjust to physical changes in the network's layout. Using RIP, the Gateway determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other Gateways on the network.
  - Transmit RIP Version. To transmit RIP messages, select the protocol you want: **RIP1, RIP1-Compatible, or RIP2**. If you don't want to transmit RIP messages, select **None**.
  - Receive RIP Version. To receive RIP messages, select the protocol you want: **RIP1** or **RIP2**. If you don't want to receive RIP messages, select **None**.
  - Multicast or Broadcast. RIP can be sent using either methods. If you want to use multicasting, select **Multicast**. If you want to use Broadcast, select **Broadcast**.
- Static Routing. If the Gateway is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To create a static route, change the following settings:

  - Select set number. Select the number of the static route from the drop-down menu. The Gateway supports up to 20 static route entries. If you need to delete a route, then select the entry and click the **Delete This Entry** button.
  - Destination IP Address. The Destination IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0.
  - Subnet Mask. Enter the Subnet Mask (also known as the Network Mask), which determines which portion of an IP address is the network portion, and which portion is the host portion.
  - Gateway. Enter the IP address of the gateway device that allows for contact between the Gateway and the remote network or host.
  - Hop Count. Hop Count is the number of hops to each node until the destination is reached (16 hops maximum). Enter the Hop Count in the field provided.
- Show Routing Table. Click the **Show Routing Table** button to open a screen displaying how data is routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click the **Refresh** button to update the information. Click the **Close** button to return to the previous screen.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Routing Table Entry List (Refresh)

Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	LAN & Wireless

(Close)

Figure 5-13: Routing Table

The Wireless Tab

The Basic Wireless Settings Tab

This screen allows you to choose your wireless network mode and wireless security.

Wireless Network

- Wireless Network Mode. If you have 802.11g and 802.11b devices in your network, then keep the default setting, **Mixed**. If you have only 802.11g devices, select **802.11g**. If you have only 802.11b devices, select **802.11b**. If you want to disable wireless networking, select **Disabled**.
- Wireless Network Name (SSID). Enter the name for your wireless network into the field. The SSID is the network name shared among all devices in a wireless network. It must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Linksys recommends that you change the default SSID (linksys) to a unique name of your choice.
- Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to function correctly. Wireless computers or clients will automatically detect the wireless channel of the Gateway.
- Wireless SSID Broadcast. When wireless computers or clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Gateway. To broadcast the Gateway's SSID, keep the default setting, **Enable**. If you do not want to broadcast the Gateway's SSID, then select **Disable**.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

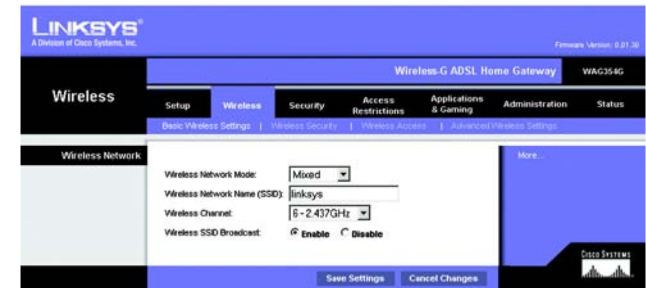


Figure 5-14: Basic Wireless Settings

The Wireless Security Tab

The Wireless Security settings configure the security of your wireless network. There are two wireless security options supported by the Gateway: WPA Pre-Shared Key and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy.) These are briefly discussed here. For detailed instructions on configuring wireless security for the Gateway, turn to "Appendix B: Wireless Security." If you want to disable wireless security, select **Disable** from the drop-down menu for Security Mode.

WPA Pre-Shared Key. Enter a WPA Shared Key of 8-32 characters. Then enter a Group Key Renewal period, which instructs the Gateway how often it should change the encryption keys.



Figure 5-15: WPA Pre-Shared Key

WEP. WEP is a basic encryption method, which is not as secure as WPA. To use WEP, select a Default Key (this indicates which Key to use) and a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Then either generate a WEP key using a Passphrase or enter the WEP key manually.

- WEP Encryption. An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode data transmissions, all devices in a network must use an identical WEP key. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance. To enable WEP, select **64 bits 10 hex digits** or **128 bits 26 hex digits**.
- Default Transmit Key Select which WEP key (1-4) will be used when the Gateway sends data. Make sure that the receiving device (wireless computer or client) is using the same key.
- Passphrase. Instead of manually entering WEP keys, you can enter a passphrase. This passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 32 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only and cannot be used with Windows XP Zero Configuration. If you want to communicate with non-Linksys wireless products or Windows XP Zero Configuration, make a note of the WEP key generated in the *Key 1* field, and enter it manually in the wireless computer or client.) After you enter the Passphrase, click the **Generate** button to create WEP keys.
- WEP Keys 1-4. WEP keys enable you to create an encryption scheme for wireless network transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes; they are not valid key values.) If you are using 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"-"9" and "A"-"F".

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. For detailed instructions on configuring wireless security for the Gateway, turn to "Appendix B: Wireless Security."



Figure 5-16: WEP

The Wireless Access Tab

Wireless Network Access

Wireless Network Access. Select **Allow All** you want all computers to have access to the wireless network. To restrict access to the network, select **Restrict Access**, and then select **Prevent** to block access for the designated computers or **Permit only** to permit access for the designated computers. Click the **Edit MAC Address Access List** button, and the *Mac Address Filter List* screen will appear.

Enter the MAC addresses of the computers you want to designate. To see a list of MAC addresses for wireless computers or clients, click the **Wireless Client MAC List** button.

The *Wireless Client MAC List* screen will list computers, their IP addresses, and their MAC addresses. Click the Refresh button to get the most up-to-date information. Click the **Enable MAC Filter** checkbox To add a specific computer to the Mac Address Filter List, click the **Enable MAC Filter** checkbox and then the **Update Filter List** button. Click the **Close** button to return to the *Wireless Client MAC List* screen.

On the *Wireless Client MAC List* screen, click the **Save Settings** button to save this list, or click the **Cancel Changes** button to remove your entries.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Figure 5-17: Wireless Network Access

MAC Address Filter List

Enter MAC Address Format: xxxxxxxxxxxx/xx:xx:xx:xx:xx:xx

MAC 01:		MAC 11:	
MAC 02:		MAC 12:	
MAC 03:		MAC 13:	
MAC 04:		MAC 14:	
MAC 05:		MAC 15:	
MAC 06:		MAC 16:	
MAC 07:		MAC 17:	
MAC 08:		MAC 18:	
MAC 09:		MAC 19:	
MAC 10:		MAC 20:	

Wireless Client MAC List

Save Settings Cancel Changes

Figure 5-18: MAC Address Filter List



Figure 5-19: Wireless Client MAC List

The Advanced Wireless Settings Tab

Advanced Wireless

On this screen you can access the advanced wireless features, including Authentication Type, Control TX Rate, Beacon Interval, DTIM Interval, Fragmentation Threshold, and RTS Threshold.



Figure 5-20: Advanced Wireless Settings

- Authentication Type. The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient do not use a WEP key for authentication but can use WEP for data encryption. To only allow Open System authentication, select **Open System**. For Shared Key authentication, the sender and recipient use a WEP key for both authentication and data encryption. To only allow Shared Key authentication, select **Shared Key**. It is recommended that this option be left in the default (Auto) mode, because some clients cannot be configured for Shared Key.

- Control Tx Rates The default transmission rate is **Auto**. The rate should be set depending on the speed of your wireless network. Select from a range of transmission speeds, or keep the default setting, **Auto**, to have the Gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Gateway and a wireless client.

- Beacon Interval. The default value is **100**. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Gateway to synchronize the wireless network.

- DTIM Interval. The default value is **1**. This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Gateway has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

- Fragmentation Threshold. This value should remain at its default setting of **2346**. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

- RTS Threshold. This value should remain at its default setting of **2347**. If you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Gateway sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

The Security Tab

This screen shows the VPN passthrough, firewall, and filter settings. Use these features to enhance the security of your network.

VPN Passthrough

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. Configure these settings so the Gateway will permit VPN tunnels to pass through.

- IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enable** button. To disable IPSec Passthrough, click the **Disable** button.

- PPPoE Passthrough. PPPoE Passthrough allows your PC(s) to use the PPPoE client software provided by your ISP. Some ISPs may request that you use this feature on the Gateway. To allow PPPoE Passthrough, click the **Enable** button. To disable PPPoE Passthrough, click the **Disable** button.

- PPTP Passthrough. Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP Passthrough, click the **Enable** button. To disable PPTP Passthrough, click the **Disable** button.

- L2TP Passthrough. Layering 2 Tunneling Protocol Passthrough is an extension of the Point-to-Point Tunneling Protocol (PPTP) used to enable the operation of a VPN over the Internet.To allow L2TP Passthrough, click the **Enable** button. To disable L2TP Passthrough, click the **Disable** button.

Firewall

You can enable or disable the firewall, select filters to block specific Internet data types, and block anonymous Internet requests.

To use the firewall, click **Enable**. If you do not want to use the firewall, click **Disable**.

Additional Filters

- Filter Proxy. Use of WAN proxy servers may compromise the Gateway's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click the checkbox.

- Filter Cookies. A cookie is data stored on your computer and used by Internet sites when you interact with them. To enable cookie filtering, click the checkbox.

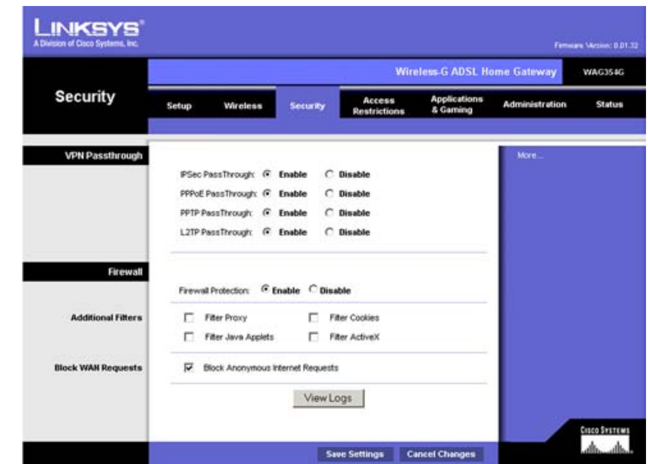


Figure 5-21: Security

- Filter Java Applets. Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using this programming language. To enable Java Applet filtering, click the checkbox.
- Filter ActiveX. ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click the checkbox.

Block WAN Requests

- Block Anonymous Internet Requests. This keeps your network from being "pinged" or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to discover your network. Select **Block Anonymous Internet Requests** to block anonymous Internet requests or de-select it to allow anonymous Internet requests.

If you want to see activity logs for your security measures, then click the **View Logs** button. Click the **Clear** button to clear the log information. Click the **pageRefresh** button to refresh the information. Click the **Previous Page** button to go to the previous page of information. Click the **Next Page** button to move to the next page of information.

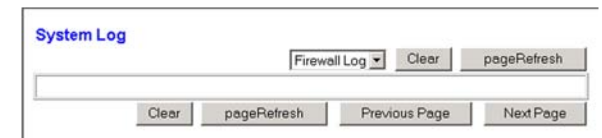


Figure 5-22: Firewall Log

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

The Access Restrictions Tab

The Internet Access Tab

The *Internet Access* screen allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific computers and block websites by URL address or keyword.

Internet Access Policy. Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the **Delete** button. To view all the policies, click the **Summary** button. (Policies can be deleted from the *Summary* screen by selecting the policy or policies and clicking the **Delete** button. To return to the Internet Access screen, click the **Close** button.)

Status. Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and click the radio button beside *Enable*.

To create an Internet Access policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, click the radio button beside *Enable*.
3. Enter a Policy Name in the field provided.

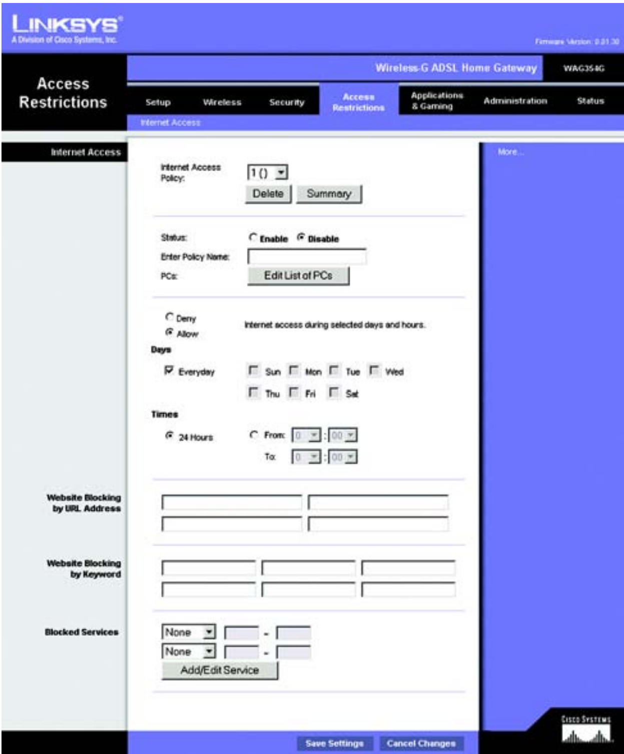


Figure 5-23: Internet Access

Internet Policy Summary

No.	Policy Name	Days	Time of Day	Delete
1.	--	S M T W T F S	--	☐
2.	--	S M T W T F S	--	☐
3.	--	S M T W T F S	--	☐
4.	--	S M T W T F S	--	☐
5.	--	S M T W T F S	--	☐
6.	--	S M T W T F S	--	☐
7.	--	S M T W T F S	--	☐
8.	--	S M T W T F S	--	☐
9.	--	S M T W T F S	--	☐
10.	--	S M T W T F S	--	☐

Close

Figure 5-24: Internet Policy Summary

4. Click the **Edit List of PCs** button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

5. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.

6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

7. If you want to block websites with specific URL addresses, enter each URL in a separate field next to *Website Blocking by URL Address*.

8. If you want to block websites using specific keywords, enter each keyword in a separate field next to *Website Blocking by Keyword*.

9. You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*.

   Then enter the range of ports you want to filter.

   If the service you want to block is not listed or you want to edit a service's settings, then click the **Add/Edit Service** button. Then the *Port Services* screen will appear.

   To add a service, enter the service's name in the *Service Name* field. Select its protocol from the *Protocol* drop-down menu, and enter its range in the *Port Range* fields. Then click the **Add** button.

   To modify a service, select it from the list on the right. Change its name, protocol setting, or port range. Then click the **Modify** button.

   To delete a service, select it from the list on the right. Then click the **Delete** button.

   When you are finished making changes on the *Port Services* screen, click the **Apply** button to save changes. If you want to cancel your changes, click the **Cancel** button. To close the *Port Services* screen and return to the *Access Restrictions* screen, click the **Close** button.

10. Click the **Save Settings** button to save the policy's settings. To undo the policy's settings, click the **Cancel Changes** button.

Figure 5-25: List of PCs

Figure 5-26: Add/Edit Service

The Applications and Gaming Tab

The Single Port Forwarding Tab

Single Port Forwarding

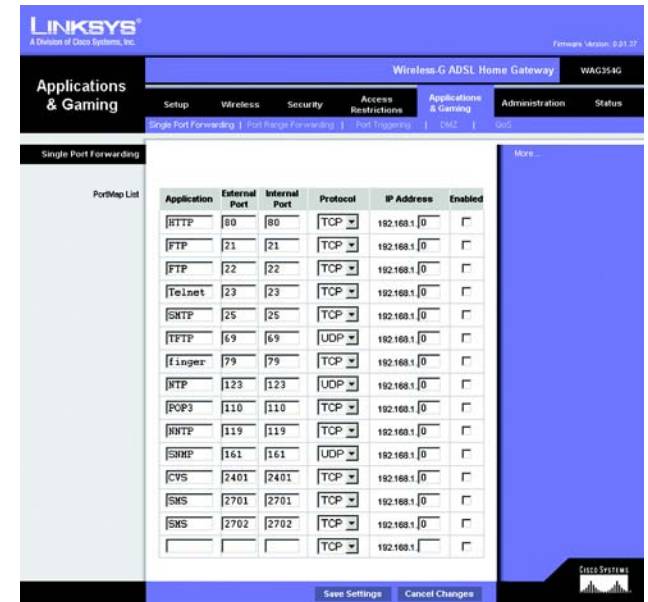


Figure 5-27: Single Port Forwarding

Use the *Single Port Forwarding* screen when you want to open a specific port so users on the Internet can see the servers behind the Gateway (such servers may include FTP or e-mail servers). When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

- Port Map List. In this section you will customize the port service for your applications.
  - Application. Enter the name of the application in the field provided.
  - External Port and Internal Port. Enter the External and Internal Port numbers.
  - Protocol. Select the protocol you wish to use for each application: **TCP** or **UDP**.
  - IP Address. Enter the IP Address of the appropriate computer.
  - Enabled. Click **Enabled** to enable forwarding for the chosen application.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

The Port Range Forwarding Tab

The *Port Range Forwarding* screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

- Application. Enter the name of the application in the field provided.
- Start and End. Enter the starting and ending numbers of the port range you wish to forward.
- Protocol. Select the protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- IP Address. Enter the IP Address of the appropriate computer.
- Enable. Click the **Enable** checkbox to enable forwarding for the chosen application.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Figure 5-28: Port Range Forwarding

The Port Triggering Tab

Port Triggering is used for special applications that can request a port to be opened on demand. For this feature, the Gateway will watch outgoing data for specific port numbers. The Gateway will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Gateway, the data is pulled back to the proper computer by way of IP address and port mapping rules.

- Application. Enter the name you wish to give each application.
- Triggered Range. Enter the starting and ending port numbers of the Triggered Range.
- Forwarded Range. Enter the starting and ending port numbers of the Forwarded Range.
- Enable. Click the **Enable** checkbox to enable port triggering for the chosen application.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Figure 5-29: Port Triggering

The DMZ Tab

The *DMZ* screen allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing through DMZ Hosting. DMZ hosting forwards all the ports for one computer at the same time, which differs from Port Range Forwarding, which can only forward a maximum of 10 ranges of ports.

- DMZ Hosting. This feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enable**. To disable DMZ, select **Disable**.
- DMZ Host IP Address. To expose one computer, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Figure 5-30: DMZ

The QoS Tab

QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as Internet phone calls or videoconferencing.

Enabled/Disabled. To use QoS, select **Enable**. Otherwise, keep the default, **Disable**.

Application-based QoS

Application-based QoS manages information as it is transmitted and received. Depending on the settings of the *QoS* screen, this feature will assign information a high or low priority for the five preset applications and three additional applications that you specify.

High priority/Medium priority/Low priority. For each application, select **High priority** (traffic on this queue shares 60% of the total bandwidth), **Medium priority** (traffic on this queue shares 18% of the total bandwidth), or **Low priority** (traffic on this queue shares 1% of the total bandwidth).

FTP (File Transfer Protocol). A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.

HTTP (HyperText Transport Protocol). The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser.

Telnet. A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

SMTP (Simple Mail Transfer Protocol). The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

POP3 (Post Office Protocol 3). A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

Specific Port#. You can add three more applications by entering their respective port numbers in these fields.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes.

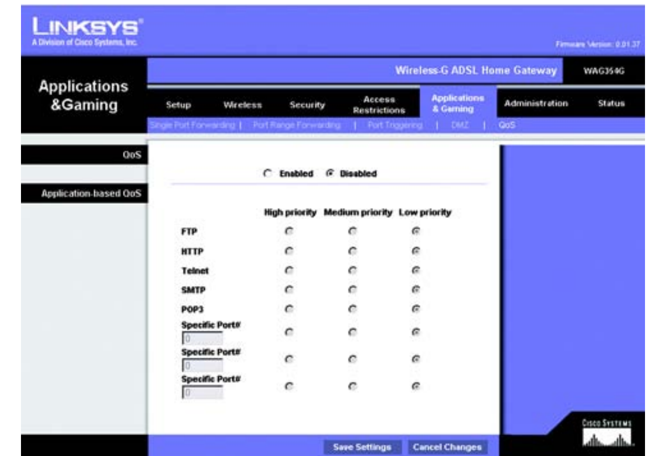


Figure 5-31: QoS

The Administration Tab

The Management Tab

The *Management* screen allows you to change the Gateway's access settings as well as configure the SNMP (Simple Network Management Protocol), UPnP (Universal Plug and Play), IGMP (Internet Group Multicast Protocol)-Proxy, and WLAN management features.

Gateway Access

Local Gateway Access. To ensure the Gateway's security, you will be asked for your password when you access the Gateway's Web-based Utility. The default username and password is **admin**.

- Gateway Userlist. Select the number of the user from the drop-down menu.
- Gateway Username. Enter the default username, **admin**. It is recommended that you change the default username to one of your choice.
- Gateway Password. It is recommended that you change the default password, **admin**, to one of your choice.
- Re-enter to confirm. Re-enter the Gateway's new Password to confirm it.

Remote Gateway Access. This feature allows you to access the Gateway from a remote location, via the Internet.

- Remote Management. This feature allows you to manage the Gateway from a remote location via the Internet. To enable Remote Management, click **Enable**.



IMPORTANT: Enabling remote management allows anyone with your password to configure the Gateway from somewhere else on the Internet.

- Management Port. Enter the port number you will use to remotely access the Gateway.
- Allowed IP. Specify the IP address(es) allowed to remotely manage the Gateway. To allow all IP addresses with no restrictions, select **All**. To specify a single IP address, select **IP address** and enter the IP address in the fields provided. To specify a range of IP addresses, select **IP range** and enter the range of IP addresses in the fields provided.

Remote Upgrade. This feature allows the Gateway's firmware to be upgraded remotely by a TFTP server. To enable Remote Upgrade, click **Enable**.

Figure 5-32: Management

Figure 5-33: Allowed IP - IP Range

SNMP

SNMP is a popular network monitoring and management protocol. To enable SNMP, click **Enabled**. To disable SNMP, click **Disabled**.

If enabled, then specify the IP address(es) allowed to have SNMP access. Select **All** to allow all IP addresses with no restrictions, **IP address** to specify a single IP address, or **IP range** to specify a range of IP addresses.

- Device Name. Enter the name of the Gateway.
- SNMP v1/v2: Get Community. Enter the password that allows read-only access to the Gateway's SNMP information.
- Set Community. Enter the password that allows read/write access to the Gateway's SNMP information.
- Trap Management: Trap to. Enter the IP address of the remote host computer that will receive the trap messages.

UPnP

UPnP allows Windows Me and XP to automatically configure the Gateway for various Internet applications, such as gaming and videoconferencing.

- UPnP. To enable UPnP, click **Enable**. Otherwise, click **Disable**.

IGMP-Proxy

If your multimedia application or device is not working properly behind the Gateway, then you can enable IGMP-Proxy to allow multicast traffic through the Gateway.

- IGMP Proxy. To use this feature, select **Enable**. Otherwise, select **Disable**.

WLAN

- Management via WLAN. This feature allows the Gateway to be managed by a wireless computer on the local network when it logs into the Gateway's Web-based Utility.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

The Reporting Tab

The *Reporting* screen provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection. It also provides logs for VPN and firewall events.



Figure 5-34: Reporting

Reporting

- Log. To enable log reporting, click **Enabled**.
- Logviewer IP Address. Enter the IP Address of the computer that will receive logs. You will need Logviewer software to view these logs. This free software is available for download from www.linksys.com.

Email Alerts

- E-Mail Alerts. To enable E-Mail Alerts, click **Enabled**.
- Denial of Service Thresholds. Enter the number of Denial of Service attacks that will trigger an e-mail alert.
- SMTP Mail Server. Enter the IP address of the SMTP server.
- E-Mail Address for Alert Logs. Enter the e-mail address that will receive alert logs.
- Return E-Mail address. Enter the return address for the e-mail alerts.

To view the logs, click the **View Logs** button. A new screen will appear. From the drop-down menu, you can select which log you want to view. Click the **Clear** button to clear the log information. Click the **pageRefresh** button to refresh the information. Click the **Previous Page** button to go to the previous page of information. Click the **Next Page** button to move to the next page of information.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Figure 5-35: System Log

The Diagnostics Tab

Ping Test

Ping Test Parameters

- Ping Target IP. Enter the IP address that you want to ping. This can be either a local (LAN) IP or an Internet (WAN) IP address.
- Ping Size. Enter the size of the packet.
- Number of Pings. Enter the number of times that you want to ping.
- Ping Interval. Enter the ping interval (how often the target IP address will be pinged) in milliseconds.
- Ping Timeout. Enter the ping timeout (how long before the ping test times out) in milliseconds.

Click the **Start Test** button to start the Ping Test.

- Ping Result. The results of the ping test will be shown here.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Figure 5-36: Ping Test

The Backup&Restore Tab

The Backup&Restore tab allows you to back up and restore the Gateway's configuration file.

Backup Configuration

To back up the Gateway's configuration file, click the **Backup** button. Then follow the on-screen instructions.

Restore Configuration

To restore the Gateway's configuration file, click the **Browse** button. Then follow the on-screen instructions to locate the file. After you have selected the file, click the **Restore** button.

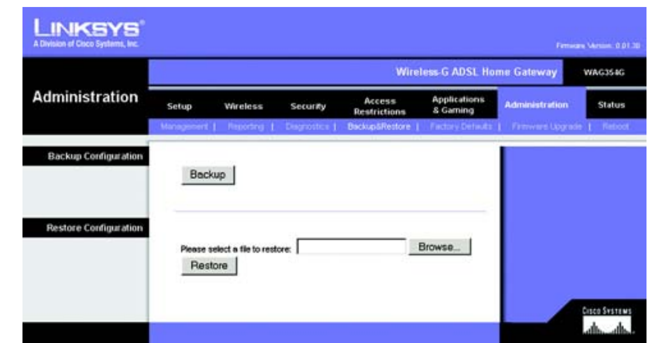


Figure 5-37: Backup&Restore

The Factory Defaults Tab

Restore Factory Defaults. If you wish to restore the Gateway to its factory default settings and lose all your settings, click **Yes**.

To begin the restore process, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Figure 5-38: Factory Defaults

The Firmware Upgrade Tab

The Gateway allows you to upgrade firmware from the LAN (Local Area Network) side of the Gateway.

Upgrade from LAN

To upgrade the Gateway's firmware from the LAN:

1. Download the Gateway's firmware upgrade file from www.linksys.com/international.
2. Extract the file on your computer.
3. Click the **Browse** button to find the firmware upgrade file.
4. Double-click the firmware file that you have downloaded and extracted.
5. Click the **Upgrade** button, and follow the on-screen instructions.

To cancel the firmware upgrade, click the **Cancel Upgrades** button.



Figure 5-39: Firmware Upgrade

The Reboot Tab



Figure 5-40: Reboot

This screen allows you to do a soft or hard reboot of the Gateway. In most cases you should use the hard reboot. The soft reboot is similar to restarting your computer without physically powering down the computer.

Reboot

Reboot Mode. To reboot your Gateway, select **Hard** or **Soft**. Choose **Hard** to power cycle the Gateway or **Soft**. to restart it without a power cycle.

To begin the reboot process, click the **Save Settings** button. When a screen appears asking you if you really want to reboot the Gateway, click **OK**.

Click the **Cancel Changes** button if you want to cancel the reboot.

The Status Tab

The Gateway Tab

This screen displays information about the Gateway and its Internet connection.

Gateway Information

This section displays the Gateway's Firmware Version, MAC Address, and Current Time.

Internet Connection

This section shows the following information: the Connection, Login Type, Interface, IP Address, Subnet Mask, Default Gateway, DNS 1, 2, and 3 server IP addresses, and WINS address.

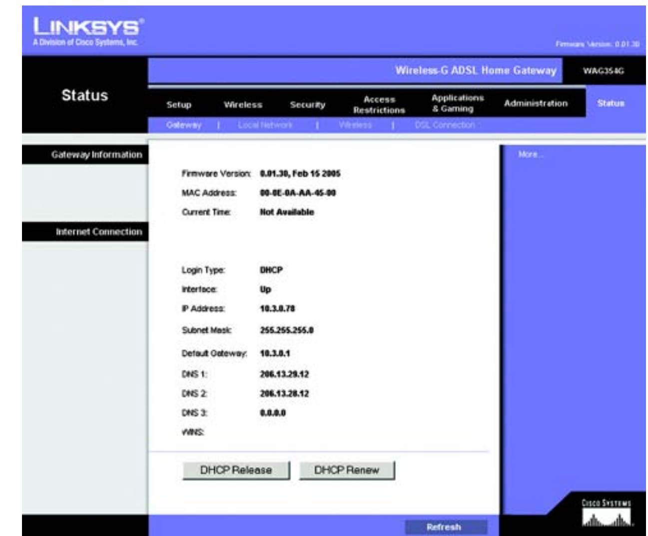


Figure 5-41: Gateway

DHCP Renew. Click the **DHCP Renew** button to replace the Gateway's current IP address with a new IP address.

DHCP Release. Click the **DHCP Release** button to delete the Gateway's current IP address.

Click the **Refresh** button if you want to refresh the displayed information.

The Local Network Tab

The Local Network information that is displayed is the local Mac Address, IP Address, Subnet Mask, DHCP Server, Start IP Address, and End IP Address. To view the DHCP Clients Table, click the **DHCP Clients Table** button. To view the ARP/RARP Table, click the **ARP/RARP Table** button.

DHCP Clients Table. The DHCP Active IP Table shows the current DHCP Client data. You will see the computer name, IP address, MAC address, and expiration time of the dynamic IP address for the wireless clients using the DHCP server. (This data is stored in temporary memory and changes periodically.) Click the **Refresh** button if you want to refresh the displayed information. To delete a client from the DHCP server, select the client, and then click the **Delete** button. Click the **Close** button to return to the *Local Network* screen.

ARP/RARP Table. The ARP/RARP Table shows the current data for the local network clients that have sent an ARP request to the Gateway. You will see their IP addresses and MAC addresses. (This data is stored in temporary memory and changes periodically.) An ARP request is a request sent by the Gateway asking clients with IP addresses for their MAC addresses, so the Gateway can map IP addresses to MAC addresses. RARP is the reverse of ARP. Click the **Refresh** button if you want to refresh the displayed information. Click the **Close** button to return to the *Local Network* screen.

Click the **Refresh** button if you want to refresh the displayed information.



Figure 5-42: Local Network

DHCP Active IP Table

DHCP Server IP Address: 192.168.1.1

Client Host Name	IP Address	MAC Address	Expires
None	None	None	None

Refresh / Delete / Close

Figure 5-43: DHCP Active IP Table

ARP/RARP Table

IP Address	MAC Address
192.168.1.64	00:D0:B7:B6:46:BA

Close / Refresh

Figure 5-44: ARP/RARP Table

The Wireless Tab

The Wireless network information that is displayed is the Wireless Firmware Version, MAC Address, Mode, SSID, DHCP Server, Channel, and Encryption Function.

Click the **Wireless Clients Connected** button to view a list of the wireless clients connected to the Gateway, along with their computer names, IP addresses, and MAC addresses. Click the **Refresh** button if you want to refresh the displayed information. Click the **Close** button to return to the *Wireless* screen.

Click the **Refresh** button if you want to refresh the displayed information.



Figure 5-45: Wireless



Figure 5-46: Networked Computers

The DSL Connection Tab

This screen shows information about the DSL connection and the PVC connection.

DSL Status

This section shows the following: DSL Status, DSL Modulation Mode, DSL Path Mode, Downstream Rate, Upstream Rate, Downstream Margin, Upstream Margin, Downstream Line Attenuation, Upstream Line Attenuation, Downstream Transmit Power, and Upstream Transmit Power.

PVC Connection

This section displays the following information: Encapsulation, Multiplexing, QoS, Pcr Rate, Scr Rate, Autodetect, VPI, VCI, Enable status, and PVC Status.

Click the **Refresh** button if you want to refresh the displayed information.



Figure 5-47: DSL Connection

Appendix A: Troubleshooting

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems that may occur during the installation and operation of the Gateway. Read the descriptions below to help you solve your problems. If you can't find an answer here, check the Linksys international website at www.linksys.com/international.

Common Problems and Solutions

1. I need to set a static IP address on a computer.

You can assign a static IP address to a computer by performing the following steps:

- For Windows 98 and Me:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
  2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the Properties button.
  3. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway. Make sure that each IP address is unique for each computer or network device.
  4. Click the **Gateway** tab, and in the New Gateway prompt, enter 192.168.1.1, which is the default IP address of the Gateway. Click the Add button to accept the entry.
  5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
  6. Click the **OK** button in the TCP/IP properties window, and click Close or the OK button for the Network window.
  7. Restart the computer when asked.
- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
  3. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
  5. Enter the Subnet Mask, 255.255.255.0.
  6. Enter the Default Gateway, 192.168.1.1 (Gateway's default IP address).

7. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
9. Restart the computer if asked.

- For Windows XP:

  The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. Click **Start** and **Control Panel**.
2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the Properties option.
4. In the **This connection uses the following items** box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
5. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
6. Enter the Subnet Mask, 255.255.255.0.
7. Enter the Default Gateway, 192.168.1.1 (Gateway's default IP address).
8. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

2. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

- Refer to Windows Help for details. Make sure Obtain IP address automatically is selected in the settings.

For Windows NT 4.0:

- Click **Start**, **Setting**s, and **Control Panel**. Double-click the **Network** icon.
- Click the Protocol tab, and double-click on TCP/IP Protocol.
- When the window appears, make sure you have selected the correct Adapter for your Ethernet adapter and set it for **Obtain an IP address** from a DHCP server.
- Click the **OK** button in the TCP/IP Protocol Properties window, and click the **Close** button in the Network window.
- Restart the computer if asked.

B. Open a command prompt.

For Windows 98 and Me:

- Click **Start** and **Run**. In the Open field, type in command. Press the **Enter** key or click the **OK** button.

For Windows NT, 2000, and XP:

- Click **Start** and **Run**. In the Open field, type cmd. Press the **Enter** key or click the **OK** button. In the command prompt, type ping 192.168.1.1 and press the Enter key.
- If you get a reply, the computer is communicating with the Gateway.
- If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.

C. In the command prompt, type ping followed by your Internet or WAN IP address and press the **Enter** key. The Internet or WAN IP Address can be found on the Status screen of the Gateway's web-based utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter ping 1.2.3.4 and press the Enter key.

- If you get a reply, the computer is connected to the Gateway.
- If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

D. In the command prompt, type ping www.yahoo.com and press the **Enter** key.

- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

3. I am not getting an IP address on the Internet with my Internet connection.

- Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
  1. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, or RFC 2364 PPPoA. Please refer to the Setup section of "Chapter 5: Configuring the Wireless-G ADSL Home Gateway" for details on Internet connection settings.
  2. Make sure you have the right cable. Check to see if the Gateway column has a solidly lit ADSL LED.
  3. Make sure the cable connecting from your Gateway's ADSL port is connected to the wall jack of the ADSL service line. Verify that the Status page of the Gateway's web-based utility shows a valid IP address from your ISP.
  4. Turn off the computer and Gateway. Wait 30 seconds, and then turn on the Gateway, and computer. Check the Status tab of the Gateway's web-based utility to see if you get an IP address.

4. I am not able to access the Setup page of the Gateway's web-based utility.

- Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Gateway.
  1. Refer to "Appendix C: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
  2. Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."

3. Refer to "Problem #10: I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window."

5. *I can't get my Virtual Private Network (VPN) working through the Gateway.*

Access the Gateway's web interface by going to http://192.168.1.1 or the IP address of the Gateway, and go to the Security tab. Make sure you have IPsec passthrough and/or PPTP pass-through enabled.

- VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Gateway; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.
- VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Gateway. AH has limitations due to occasional incompatibility with the NAT standard.
- Change the IP address for the Gateway to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Gateway will have difficulties routing information to the right location. If you change the Gateway's IP address to 192.168.2.1, that should solve the problem. Change the Gateway's IP address through the Setup tab of the web interface.
- If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.
- Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.
- Check the Linksys international website for more information at www.linksys.com/international.

6. *I need to set up a server behind my Gateway and make it available to the public.*

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed.

- Follow these steps to set up port forwarding through the Gateway's web-based utility. We will be setting up web, ftp, and mail servers.
  1. Access the Gateway's web-based utility by going to http://192.168.1.1 or the IP address of the Gateway. Go to the Applications and Gaming => Port Range Forwarding tab.
  2. Enter any name you want to use for the Customized Application.
  3. Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
  4. Check the protocol you will be using, TCP and/or UDP.
  5. Enter the IP address of the computer or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the

field provided. Check “Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter” for details on getting an IP address.

6. Check the Enable option for the port services you want to use. Consider the example below:

Customized Application	External Port	TCP	UDP	IP Address	Enable
Web server	80 to 80	X		192.168.1.100	X
FTP server	21 to 21	X		192.168.1.101	X
SMTP (outgoing)	25 to 25	X		192.168.1.102	X
POP3 (incoming)	110 to 110	X		192.168.1.102	X

When you have completed the configuration, click the **Save Settings** button.

7. ***I need to set up online game hosting or use other Internet applications.***

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Gateway to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

1. Access the Gateway’s web interface by going to http://192.168.1.1 or the IP address of the Gateway. Go to the Applications and Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the Customized Application.
3. Enter the External Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the computer or network device that you want the port server to go to. For example, if the web server’s Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check “Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter” for details on getting an IP address.
6. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized Application	External Port	TCP	UDP	IP Address	Enable
UT	7777 to 27900	X	X	192.168.1.100	X
Halflife	27015 to 27015	X	X	192.168.1.105	X
PC Anywhere	5631 to 5631		X	192.168.1.102	X
VPN IPSEC	500 to 500		X	192.168.1.100	X

When you have completed the configuration, click the **Save Settings** button.

8. ***I can't get the Internet game, server, or application to work.***

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one computer to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Gateway will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Gateway will send the data to whichever computer or network device you set for DMZ hosting.)

- Follow these steps to set DMZ hosting:
  1. Access the Gateway's web-based utility by going to http://192.168.1.1 or the IP address of the Gateway. Go to the Applications and Gaming => DMZ tab. Click Enabled and enter the IP of the computer.
  2. Check the Port Forwarding pages and disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
- Once completed with the configuration, click the **Save Settings** button.

9. ***I forgot my password, or the password prompt always appears when I am saving settings to the Gateway.***

- Reset the Gateway to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:
  1. Access the Gateway's web-based utility by going to http://192.168.1.1 or the IP address of the Gateway. Enter the default username and password **admin**, and click the **Administrations** => **Management** tab.
  2. Enter a different password in the Gateway Password field, and enter the same password in the second field to confirm the password.
  3. Click the **Save Settings** button.

10. ***I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.***

If you have proxy settings, you need to disable these on your computer. Because the Gateway is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

- For Microsoft Internet Explorer 5.0 or higher:
  1. Click **Start, Settings**, and **Control Panel**. Double-click Internet Options.
  2. Click the **Connections** tab.
  3. Click the **LAN settings** button and remove anything that is checked.
  4. Click the **OK** button to go back to the previous screen.
  5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

- For Netscape 6 or higher:
  1. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
  2. Make sure you have Direct connection to the Internet selected on this screen.
  3. Close all the windows to finish.

11. To start over, I need to set the Gateway to factory default.

Hold the **Reset** button for 10 seconds and then release it. This will return the Internet settings, password, forwarding, and other settings on the Gateway to the factory default settings. In other words, the Gateway will revert to its original factory configuration.

12. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys international website and download the latest firmware at www.linksys.com/international.

- Follow these steps:
  1. Go to the Linksys international website at http://www.linksys.com/international and select your region or country.
  2. Click the **Products** tab and select the Gateway.
  3. On the Gateway's webpage, click **Firmware**, and then download the latest firmware for the Gateway.
  4. To upgrade the firmware, follow the steps in the Administration section found in "Chapter 5: Configuring the Wireless-G ADSL Home Gateway."

13. The firmware upgrade failed, and/or the Power LED is flashing.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Power LED stop flashing:

- If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- Set a static IP address on the computer; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:
  IP Address: 192.168.1.50
  Subnet Mask: 255.255.255.0
  Gateway: 192.168.1.1
- Perform the upgrade using the TFTP program or the Gateway's web-based utility through its Administration tab.

14. My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet.

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

1. To connect to the Gateway, go to the web browser, and enter http://192.168.1.1 or the IP address of the Gateway.
2. Enter the username and password, if asked. (The default username and password is admin.)
3. On the Setup screen, select the option **Keep Alive**, and set the Redial Period option at 20 (seconds).
4. Click the **Save Settings** button. Click the **Status** tab, and click the **Connect** button.
5. You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
6. Click the **Save Settings** button to continue.

- If the connection is lost again, follow steps 1- 6 to re-establish connection.

15. *I can't access my e-mail, web, or VPN, or I am getting corrupted data from the Internet.*

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set automatically.

- If you are having some difficulties, perform the following steps:
  1. To connect to the Gateway, go to the web browser, and enter http://192.168.1.1 or the IP address of the Gateway.
  2. Enter the username and password, if asked. (The default username and password is admin.)
  3. Look for the MTU option, and select **Manual**. In the Size field, enter 1492.
  4. Click the **Save Settings** button to continue.
- If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
  1462
  1400
  1362
  1300

16. *The Power LED flashes continuously.*

The Power LED lights up when the device is first powered up. In the meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED remains steady to show that the system is working fine. If the LED continues to flash after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0.

17. *When I enter a URL or IP address, I get a time-out error or am prompted to retry.*

- Check if other computers work. If they do, ensure that your computer's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the computers are configured correctly, but still not working, check the Gateway. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)

- If the Gateway is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Gateway to verify a direct connection.
- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

18. I'm trying to access the Gateway's Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, "404 Forbidden."

If you are using Windows Explorer, perform the following steps until you see the Web-based Utility's login screen (Netscape Navigator will require similar steps):

1. Click **File**. Make sure *Work Offline* is NOT checked.
2. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.

- Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

Frequently Asked Questions

What is the maximum number of IP addresses that the Gateway will support?

The Gateway will support up to 253 IP addresses.

Is IPSec Passthrough supported by the Gateway?

Yes, it is a built-in feature that is enabled by default.

Where is the Gateway installed on the network?

In a typical environment, the Gateway is installed between the ADSL wall jack and the LAN.

Does the Gateway support IPX or AppleTalk?

No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to a LAN.

Does the LAN connection of the Gateway support 100Mbps Ethernet?

The Gateway supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Gateway.

What is Network Address Translation and what is it used for?

Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a computer connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Gateway to be used with low cost Internet accounts when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Gateway support any operating system other than Windows 98SE, Windows Millennium, Windows 2000, or Windows XP?

Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

Does the Gateway support ICQ send file?

Yes, with the following fix: click ICQ menu -> preference -> connections tab->, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the Gateway.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?

If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Gateway from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?

It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get Half-Life: Team Fortress to work with the Gateway?

The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?

Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at www.linksys.com/international for more information.

If all else fails in the installation, what can I do?

Reset the Gateway by holding down the reset button until the Power LED fully turns on and off. Reset your DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys international website, www.linksys.com/international.

How will I be notified of new Gateway firmware upgrades?

All Linksys firmware upgrades are posted on the Linksys international website at www.linksys.com/international, where they can be downloaded for free. To upgrade the Gateway's firmware, use the Administration tab of the Gateway's web-based utility. If the Gateway's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use.

Will the Gateway function in a Macintosh environment?

Yes, but the Gateway's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Gateway. What can I do?

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

What is DMZ Hosting?

Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

If DMZ Hosting is used, does the exposed user share the public IP with the Gateway?

No.

Does the Gateway pass PPTP packets or actively route PPTP sessions?

The Gateway allows PPTP packets to pass through.

Is the Gateway cross-platform compatible?
Any platform that supports Ethernet and TCP/IP is compatible with the Gateway.

How many ports can be simultaneously forwarded?
Theoretically, the Gateway can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

What are the advanced features of the Gateway?
The Gateway's advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing, and DDNS.

What is the maximum number of VPN sessions allowed by the Gateway?
The maximum number depends on many factors. At least one IPSec session will work through the Gateway; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

How can I check whether I have static or DHCP IP Addresses?
Consult your ISP to obtain this information.

How do I get mIRC to work with the Gateway?
Under the Port Forwarding tab, set port forwarding to 113 for the computer on which you are using mIRC.

Can the Gateway act as my DHCP server?
Yes. The Gateway has DHCP server software built-in.

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

What IEEE 802.11b and 802.11g features are supported?

The product supports the following IEEE 802.11b and IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

It also supports OFDM technology for 802.11g networking.

What is ad-hoc mode?

When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other, peer-to-peer without the use of an access point.

What is infrastructure mode?

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a network through a wireless access point.

What is roaming?

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the computer must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is the ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Will the information be intercepted while it is being transmitted through the air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I reset the Gateway?

Press the Reset button on the back panel for about ten seconds. This will reset the Gateway to its default settings.

How do I resolve issues with signal loss?

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Gateway and a wireless computer will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Gateway and your wireless computer in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel.

I have excellent signal strength, but I cannot see my network.

WEP is probably enabled on the Gateway, but not on your wireless adapter (or vice versa). Verify that the same WEP keys and levels (64 or 128) are being used on all nodes of your wireless network.

How many channels/frequencies are available with the Gateway?

There are eleven available channels, ranging from 1 to 11, in North America. There may be additional channels available in other regions, subject to the regulations of your region and/or country.

If your questions are not addressed here, refer to the Linksys international website, www.linksys.com/international.

Appendix B: Wireless Security

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

Security Precautions

The following is a complete list of security precautions to take (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

For information on implementing these security features, refer to “Chapter 6: Configuring the Wireless-G ADSL Home Gateway.”



NOTE: Some of these security features are available only through the network gateway, router, or access point. Refer to the gateway, router, or access point’s documentation for more information.

Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for “beacon messages”. These messages can be easily decrypted and contain much of the network’s information, such as the network’s SSID (Service Set Identifier). Here are the steps you can take:

Change the administrator’s password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator’s password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator’s password regularly.

SSID. There are several things to keep in mind about the SSID:

1. Disable Broadcast
2. Make it unique
3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

MAC Addresses. Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

WEP Encryption. Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible
2. Use "Shared Key" authentication
3. Change your WEP key regularly

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.



IMPORTANT: Always remember that each device in your wireless network MUST use the same encryption method and encryption key or your wireless network will not function properly.

WPA Pre-Shared Key. If you do not have a RADIUS server, Select the type of algorithm, TKIP or AES, enter a password in the Pre-Shared key field of 8-64 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Gateway or other device how often it should change the encryption keys.

WPA RADIUS. WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Gateway or other device.) First, select the type of WPA algorithm, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

RADIUS. WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Gateway or other device.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Then, select a WEP key and a level of WEP encryption, and either generate a WEP key through the Passphrase or enter the WEP key manually.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering feature of the Gateway. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Gateway's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

Windows 98 or Me Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.

2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Gateway via a CAT 5 Ethernet network cable. See Figure C-1.

3. Write down the Adapter Address as shown on your computer screen (see Figure C-2). This is the MAC address for your Ethernet adapter and is shown in hexadecimal as a series of numbers and letters.

   The MAC address/Adapter Address is what you will use for MAC filtering. The example in Figure D-2 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

   The example in Figure C-2 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.



Note: The MAC address is also called the Adapter Address.

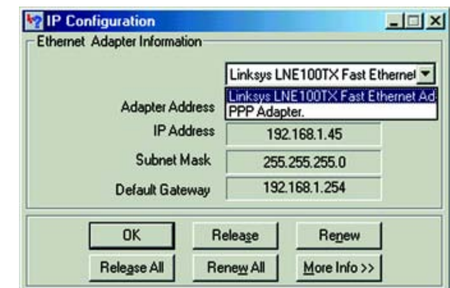


Figure C-1: IP Configuration Screen

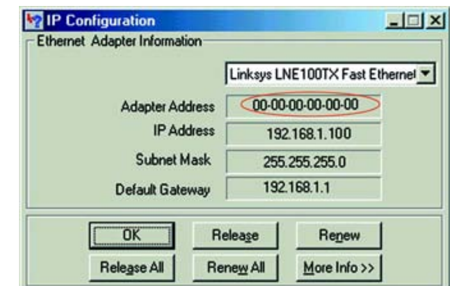


Figure C-2: MAC Address/Adapter Address

Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.



Note: The MAC address is also called the Physical Address.

2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.

3. Write down the Physical Address as shown on your computer screen (Figure C-3); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

   The MAC address/Physical Address is what you will use for MAC filtering. The example in Figure C-3 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

   The example in Figure C-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

```
C:\>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . :
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Linksys LNE100TX(v5) Fast Ethernet A
dapter
        Physical Address. . . . . . . . . : 00-00-00-00-00-00
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1

        Primary WINS Server . . . . . . . : 192.168.1.1
        Secondary WINS Server . . . . . . :
        Lease Obtained. . . . . . . . . . : Monday, February 11, 2002 2:31:47 PM

        Lease Expires . . . . . . . . . . : Tuesday, February 12, 2002 2:31:47 P
M

C:\>
```

Figure C-3: MAC Address/Physical Address

Appendix D: Upgrading Firmware

To upgrade the Gateway's firmware:

1. Download the Gateway's firmware upgrade file from *www.linksys.com/international*.
2. Extract the file on your computer.
3. Open the Gateway's Web-based Utility and click the **Administration** tab.
4. Click the **Firmware Upgrade** tab.
5. Click the **Browse** button to find the extracted file, and then double-click it.
6. Click the **Upgrade** button, and follow the on-screen instructions.



Figure D-1: Firmware Upgrade

Appendix E: Glossary

802.11b - A wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - A wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - A device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

AES (**A**dvanced **E**ncryption **S**tandard) - A security method that uses symmetric 128-bit block data encryption.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects different networks.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

Buffer - A shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other.

Byte - A unit of data that is usually eight bits long

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

CTS (**C**lear **T**o **S**end) - A signal sent by a wireless device, signifying that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**D**e**mil**itarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP (**E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity) - A mutual authentication method that uses digital certificates.

Encryption - Encoding data transmitted in a network.

Ethernet - A networking protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

Fragmentation -Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a username and password system.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

mIRC - An Internet Relay Chat program that runs under Windows.

Multicasting - Sending data to a group of destinations at once.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) - Frequency transmission that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel to prevent information from being lost in transit.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

PEAP (**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack-**45**) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (**R**equest **T**o **S**end) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (**U**ser **D**atagram **P**rotocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VPN (**V**irtual **P**rivate **N**etwork) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (**W**ide **A**rea **N**etwork)- The Internet.

WEP (**W**ired **E**quivalent **P**rivacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Me utility that displays the IP address for a particular networking device.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix F: Regulatory Information

Compliance Information for 2.4-GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

Declaration of Conformity with Regard to the EU Directive 1995/5/EC (R&TTE Directive)

NOTE: For all products, the Declaration of Conformity is available through one or more of these options:

- A pdf file is included on the product's CD.
- A print copy is included with the product.
- A pdf file is available on the product's webpage. Visit www.linksys.com/international and select your country or region. Then select your product.

If you need any other technical documentation, see the "Technical Documents on www.linksys.com/international" section, as shown later in this appendix.

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 300 328
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950

CE Marking

For the Linksys Wireless-B and Wireless-G products, the following CE mark, notified body number (where applicable), and class 2 identifier are added to the equipment.

CE 0560 ⓘ or CE 0678 ⓘ or CE ⓘ

Check the CE label on the product to find out which notified body was involved during the assessment.

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

France

In case the product is used outdoors, the output power is restricted in some parts of the band. See Table 1 or check http://www.art-telecom.fr/ for more details.

Dans la cas d’une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous à la table 1 ou visitez http://www.art-telecom.fr/ pour de plus amples détails.

Table 1: Applicable Power Levels in France

Location	Frequency Range (MHz)	Power (EIRP)
Indoor (No restrictions)	2400-2483.5	100 mW (20 dBm)
Outdoor	2400-2454 2454-2483.5	100 mW (20 dBm) 10 mW (10 dBm)

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless operating within the boundaries of the owner’s property, the use of this 2.4 GHz Wireless LAN product requires a ‘general authorization’. Please check with http://www.comunicazioni.it/it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all’interno del proprio fondo, l’utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una “Autorizzazione Generale”. Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Product Usage Restrictions

This product is designed for indoor usage only. Outdoor usage is not recommended. Any modification or alteration to the product shall void the warranty (see the Warranty Information appendix in this User Guide).

This product is designed for use with the standard, integral or dedicated (external) antenna(s) that is/are shipped together with the equipment. However, some applications may require the antenna(s) to be separated from the product and installed remotely from the device by using extension cables. For these applications, Linksys offers an R-SMA extension cable (AC9SMA) and an R-TNC extension cable (AC9TNC). Both of these cables are 9 meters long and have a cable loss (attenuation) of 5 dB. To compensate for the attenuation, Linksys also offers higher gain antennas, the HGA7S (with R-SMA connector) and HGA7T (with R-TNC connector). These antennas have a gain of 7 dBi and may only be used with either the R-SMA or R-TNC extension cable.

Combinations of extension cables and antennas resulting in a radiated power level exceeding 100 mW EIRP are illegal.

Power Output of Your Device

To comply with your country's regulations, you may have to change the power output of your wireless device. Proceed to the appropriate section for your device.

Note: The power output setting may not be available on all wireless products. For more information, refer to the documentation on your product's CD or http://www.linksys.com/international.

Wireless Adapters

Wireless adapters have the power output set to 100% by default. Maximum power output on each adapter does not exceed 20 dBm (100 mW); it is generally 18 dBm (64 mW) or below. If you need to alter your wireless adapter's power output, follow the appropriate instructions for your computer's Windows operating system:

Windows XP
1. Double-click the **Wireless** icon in your desktop's system tray.
2. Open the *Wireless Network Connection* window.
3. Click the **Properties** button.
4. Select the **General** tab, and click the **Configure** button.
5. In the *Properties* window, click the **Advanced** tab.
6. Select **Power Output**.
7. From the pull-down menu on the right, select the wireless adapter's power output percentage.

Windows 2000
1. Open the **Control Panel**.
2. Double-click **Network and Dial-Up Connections**.
3. Select your current wireless connection, and select **Properties**.
4. From the *Properties* screen, click the **Configure** button.
5. Click the **Advanced** tab, and select **Power Output**.
6. From the pull-down menu on the right, select the wireless adapter's power setting.

If your computer is running Windows Millennium or 98, then refer to Windows Help for instructions on how to access the advanced settings of a network adapter.

Wireless Access Points, Routers, or Other Wireless Products

If you have a wireless access point, router or other wireless product, use its Web-based Utility to configure its power output setting (refer to the product's documentation for more information).

Technical Documents on www.linksys.com/international

Follow these steps to access technical documents:

1. Browse to http://www.linksys.com/international.
2. Click the region in which you reside.
3. Click the name of the country in which you reside.
4. Click **Products**.
5. Click the appropriate product category.
6. Select a product.
7. Click the type of documentation you want. The document will automatically open in PDF format.

Note: If you have questions regarding the compliance of these products or you cannot find the information you need, please contact your local sales office or visit http://www.linksys.com/international for more details.

Appendix G: Warranty Information

Linksys warrants to You that, for a period of three years (the “Warranty Period”), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS’ LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

This Warranty is valid and may be processed only in the country of purchase.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix H: Specifications

Model Number	WAG354G
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, G.992.1 (G.dmt), G.992.2 (G.lite), G.992.3, G.992.5, T1.413i2
Ports	Power, ADSL, Ethernet (1-4)
Button	One Reset Button
Cabling Type	CAT 5 UTP
LEDs	Power, Wireless, Ethernet (1-4), DSL, Internet
Transmit Power	18 dBm
Channels	13 (most of Europe)
UPnP able/cert	Able
Security Features	Password protected configuration for web access PAP and CHAP authentication Denial of Service (DoS) Prevention URL filtering, and keyword, Java, ActiveX, Proxy, Cookie blocking ToD filter (Blocks Access by Time) VPN Passthrough for IPSec, PPTP, and L2TP Protocols 128, 64 bits WEP with Passphrase WEP key generation SSID Broadcast Disable Access restriction by MAC and IP addresses
WEP Key Bits	64, 128

Dimensions	140 mm x 140 mm x 27 mm (5,51" x 5,51" x 1,06")
Unit Weight	0,3 kg (0,6 lb.)
Power	12VDC 1A
Certifications	CE
Operating Temp.	0º~40ºC (32º~104ºF)
Storage Temp.	-20º~70ºC (-4º~158ºF)
Operating Humidity	10~85% Non-Condensing
Storage Humidity	5~90% Non-Condensing

Appendix I: Contact Information

Need to contact Linksys?
Visit us online for information on the latest products and updates to your existing products at:
http://www.linksys.com/international

If you experience problems with any Linksys product, you can e-mail us at:

In Europe	E-mail Address
Austria	support.at@linksys.com
Belgium	support.be@linksys.com
Denmark	support.dk@linksys.com
France	support.fr@linksys.com
Germany	support.de@linksys.com
Italy	support.it@linksys.com
Netherlands	support.nl@linksys.com
Norway	support.no@linksys.com
Portugal	support.pt@linksys.com
Spain	support.es@linksys.com
Sweden	support.se@linksys.com
Switzerland	support.ch@linksys.com
United Kingdom & Ireland	support.uk@linksys.com

Outside of Europe	E-mail Address
Latin America	support.la@linksys.com
U.S. and Canada	support@linksys.com





2,4 GHz 802.11g **Wireless-G**



ADSL-Home-Gateway

Benutzerhandbuch



Modell-Nr. **WAG354G (DE)**

Copyright und Marken

Hinweise zur Verwendung dieses Handbuchs

Ziel des Benutzerhandbuchs zum Wireless-G ADSL-Home-Gateway ist, Ihnen den Einstieg in den Netzwerkbetrieb mit dem Gateway noch weiter zu erleichtern. Achten Sie beim Lesen dieses Benutzerhandbuchs auf Folgendes:



Dieses Häkchen kennzeichnet einen Hinweis, den Sie bei Verwendung des Gateways besonders beachten sollten.



Dieses Ausrufezeichen kennzeichnet eine Warnung und weist darauf hin, dass unter bestimmten Umständen Schäden an Ihrem Eigentum oder am Gateway verursacht werden können.



Dieses Fragezeichen dient als Erinnerung an bestimmte Schritte, die bei Verwendung des Gateways durchzuführen sind.

Neben den Symbolen finden Sie Definitionen für technische Begriffe, die in folgender Form dargestellt werden:

Begriff: *Definition.*

Alle Abbildungen (Diagramme, Bildschirmdarstellungen und andere Bilder) sind mit einer Abbildungsnummer und einer Kurzbeschreibung versehen (siehe folgendes Beispiel):

Abbildung 0-1: Kurzbeschreibung der Abbildung

Die Abbildungsnummern und die zugehörigen Kurzbeschreibungen finden Sie auch im Inhaltsverzeichnis unter „Abbildungsverzeichnis“.

WAG354G-DE-UG-50516A JL

Inhaltsverzeichnis

Abbildungsverzeichnis

Kapitel 1: Einführung

Willkommen

Vielen Dank, dass Sie sich für ein Wireless-G ADSL-Home-Gateway entschieden haben. Mit diesem Gateway stehen Ihren Computern eine High Speed-Internetverbindung und Ressourcen wie beispielsweise Dateien und Drucker zur Verfügung. Da es sich um ein Wireless-Gateway handelt, kann der Internetzugriff sowohl über das verdrahtete Netzwerk als auch als Wireless-Übertragung mit bis zu 11 Mbit/s für Wireless-B bzw. 54 Mbit/s für Wireless-G erfolgen.

Wie schafft das Gateway das? Wenn das Gateway mit dem Internet sowie Computern und Peripheriegeräten verbunden wird, kann die Netzwerkkommunikation durch das Gateway gesteuert und überwacht werden.

Das Gateway verfügt zum Schutz Ihrer Daten und Ihrer Privatsphäre über eine verbesserte Firewall, mit der Eindringlinge aus dem Internet abgewehrt werden. Wireless-Datenübertragungen können durch leistungsstarke Datenverschlüsselung geschützt werden. Zudem können Sie Ihre Familie mit Kinderschutzfunktionen wie dem Einschränken der Internetzugriffszeiten und dem Blockieren von Schlüsselwörtern schützen. Die Gateway-Einstellungen können über das benutzerfreundliche, browserbasierte Dienstprogramm konfiguriert werden.

Und was genau bedeutet das?

Mit Netzwerken können Sie einen Internetzugang und Computer-Ressourcen gemeinsam mit anderen nutzen. Sie können von verschiedenen Computern aus auf einem Drucker drucken und auf Daten zugreifen, die auf der Festplatte eines anderen Computers gespeichert sind. Netzwerke eignen sich darüber hinaus auch für Videospiele mit mehreren Spielern. Netzwerke sind also nicht nur zu Hause und im Büro nützlich, sondern lassen sich auch für Unterhaltungszwecke nutzen.

Mehrere PCs in einem verdrahteten Netzwerk stellen ein LAN (*Local Area Network*; Lokales Netzwerk) dar. Sie werden über Ethernetkabel angeschlossen, daher die Bezeichnung „verdrahtetes“ Netzwerk. Mit Wireless-Karten oder -Adaptern ausgerüstete PCs können ganz ohne lästige Kabel kommunizieren. Indem sie innerhalb ihres Übertragungsradius dieselben Wireless-Einstellungen verwenden, bilden sie ein Wireless-Netzwerk. Dies wird oft als WLAN (*Wireless Local Area Network*) oder drahtloses lokales Netzwerk bezeichnet. Da das Gateway mit Wireless-Funktionen ausgestattet ist, kann es verdrahtete Netzwerke und Wireless-Netzwerke miteinander verbinden, so dass diese miteinander kommunizieren können.

Durch das Verbinden aller verdrahteten und Wireless-Netzwerke sowie des Internets können Sie jetzt Dateien gemeinsam nutzen, gemeinsam auf das Internet zugreifen und sogar Spiele spielen. Und dabei schützt das Wireless-G ADSL-Home-Gateway Ihre Netzwerke stets vor nicht autorisierten und nicht willkommenen Benutzern.

Linksys empfiehlt, für die erstmalige Installation des Gateways die Installations-CD-ROM zu verwenden. Wenn Sie den auf der Installations-CD-ROM befindlichen Installationsassistenten nicht ausführen möchten, können Sie die in diesem Handbuch aufgeführten Anleitungsschritte durchführen, um das Gateway anzuschließen, einzurichten und für die Verbindung der verschiedenen Netzwerke zu konfigurieren. Diese Anleitungen enthalten alle Informationen, die Sie zur optimalen Nutzung des Wireless-G ADSL-Home-Gateways benötigen.

WPA *(Wi-Fi Protected Access): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (Temporal Key Integrity Protocol) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann.*

SPI-Firewall *(Stateful Packet Inspection): Eine Technologie zur Überprüfung von eingehenden Datenpaketen, bevor diese an das Netzwerk weitergeleitet werden.*

Firewall*: Sicherheitsmaßnahmen, durch die die Ressourcen in einem lokalen Netzwerk vor dem Zugriff durch nicht autorisierte Dritte geschützt werden.*

NAT *(Network Address Translation): Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.*

Netzwerk: *Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam nutzen, speichern und untereinander übertragen können.*

LAN *(Local Area Network): Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr Heim- oder Büronetzwerk zusammensetzt.*

Inhalt dieses Benutzerhandbuchs

In diesem Benutzerhandbuch sind die zur Installation und Verwendung des Wireless-G ADSL-Home-Gateways erforderlichen Schritte aufgeführt.

- Kapitel 1: Einführung
  In diesem Kapitel werden die Anwendungen des Wireless-G ADSL-Home-Gateways sowie dieses Benutzerhandbuch beschrieben.

- Kapitel 2: Planen Ihres Netzwerks
  In diesem Kapitel werden die Grundlagen des Netzwerkbetriebs beschrieben.

- Kapitel 3: Beschreibung des Wireless-G ADSL-Home-Gateways
  In diesem Kapitel werden die physischen Merkmale des Gateways beschrieben.

- Kapitel 4: Anschließen des Wireless-G ADSL-Home-Gateways
  In diesem Kapitel finden Sie Anleitungen zum Anschließen des Gateways an das Netzwerk.

- Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways
  In diesem Kapitel wird erläutert, wie Sie die Einstellungen des Gateways mithilfe des webbasierten Dienstprogramms konfigurieren.

- Anhang A: Fehlerbehebung
  In diesem Anhang werden einige Probleme und Lösungsansätze sowie häufig gestellte Fragen im Zusammenhang mit der Installation und Verwendung des Wireless-G ADSL-Home-Gateways erörtert.

- Anhang B: Sicherheit im Wireless-Netzwerkbetrieb
  In diesem Anhang werden die Risiken des Wireless-Netzwerkbetriebs sowie einige Lösungen zur Eingrenzung der Risiken erklärt.

- Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters
  In diesem Anhang wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterung bzw. die Gateway-Funktion zum Kopieren von MAC-Adressen verwenden zu können.

- Anhang D: Aktualisieren der Firmware
  In diesem Anhang finden Sie eine Anleitung zum Aktualisieren der Gateway-Firmware, sollte dies einmal erforderlich sein.

- Anhang E: Glossar
  In diesem Anhang finden Sie ein kurzes Glossar mit häufig verwendeten Begriffen aus dem Bereich Netzwerkbetrieb.

- Anhang F: Zulassungsinformationen
  In diesem Anhang sind die für das Gateway geltenden Zulassungsinformationen aufgeführt.

- Anhang G: Garantieinformationen
  Dieser Anhang enthält die Garantieinformationen für das Gateway.

- Anhang H: Spezifikationen
  In diesem Anhang sind die technischen Spezifikationen des Gateways aufgeführt.

- Anhang I: Kontaktinformationen
  In diesem Anhang finden Sie Kontaktinformationen zu einer Reihe von Linksys Ressourcen, darunter auch zum Kundendienst.

Kapitel 2: Planen Ihres Netzwerks

Die Funktionen des Gateways

Ein Gateway ist ein Netzwerkgerät, das zwei Netzwerke miteinander verbindet.

In diesem Fall verbindet das Gateway Ihr lokales Netzwerk (LAN) oder die Computer zu Hause oder im Büro mit dem Internet. Das Gateway verarbeitet und lenkt die zwischen diesen beiden Netzwerken übertragenen Daten.

Mit der NAT-Funktion des Gateways wird Ihr Computernetzwerk geschützt, so dass Ihre Computer für andere Benutzer im Internet nicht „sichtbar“ sind. Somit wird der private Charakter Ihres Netzwerks bewahrt. Das Gateway schützt Ihr Netzwerk, indem es alle über den Internetanschluss eingehenden Datenpakete überprüft, bevor sie an den entsprechenden Computer in Ihrem Netzwerk geliefert werden. Das Gateway überprüft Internet-Anschlussdienste, wie z. B. den Webserver, FTP-Server oder andere Internetanwendungen, und leitet, sofern zulässig, das jeweilige Paket an den entsprechenden Computer im LAN weiter.

Beachten Sie, dass Sie über die Ports des Gateways eine Verbindung zu zwei verschiedenen Netzwerken herstellen können. Mit den LAN-Ports können Sie eine Verbindung zum LAN und mit dem ADSL-Port eine Verbindung zum Internet herstellen. Die LAN-Ports übertragen Daten mit einer Geschwindigkeit von 10/100 Mbit/s.



Abbildung 2-1: Netzwerk

IP-Adressen

Was ist eine IP-Adresse?

IP steht für *Internet Protocol* (Internet Protokoll). Jedes Gerät in einem IP-basierten Netzwerk, einschließlich Computern, Druckservern und Gateways, benötigt eine IP-Adresse, mit der sein „Standpunkt“ bzw. seine Adresse im Netzwerk identifiziert werden kann. Dies gilt sowohl für Internet- als auch für LAN-Verbindungen. Es gibt zwei Möglichkeiten, Ihren Netzwerkgeräten eine IP-Adresse zuzuweisen. Sie können statische IP-Adressen oder mithilfe des Gateways dynamische IP-Adressen zuweisen.

Statische IP-Adressen

Bei einer statischen IP-Adresse handelt es sich um eine feste IP-Adresse, die einem Computer oder einem anderen Netzwerkgerät manuell zugewiesen wird. Da eine statische IP-Adresse solange gültig ist, bis Sie sie deaktivieren, wird durch das Zuweisen einer statischen IP-Adresse sichergestellt, dass das entsprechende Gerät stets dieselbe IP-Adresse hat, bis diese geändert wird. Statische IP-Adressen müssen eindeutig sein und werden im Allgemeinen bei Netzwerkgeräten, wie z. B. Server-Computern oder Druckservern, verwendet.

IP *(Internet Protocol): Ein Protokoll, mit dem Daten über Netzwerke gesendet werden.*



HINWEIS: Da es sich bei dem Gateway um ein Gerät handelt, mit dem zwei Netzwerke verbunden werden, sind zwei IP-Adressen erforderlich, eine für das LAN und eine für das Internet. In diesem Benutzerhandbuch wird auf „Internet-IP-Adressen“ und „LAN-IP-Adressen“ verwiesen.

Da bei dem Gateway NAT-Technologie eingesetzt wird, ist die einzige IP-Adresse Ihres Netzwerks, die vom Internet aus sichtbar ist, die Internet-IP-Adresse des Gateways. Es kann jedoch auch diese Internet-IP-Adresse blockiert werden, so dass Gateway und Netzwerk für das Internet unsichtbar sind. Weitere Informationen hierzu finden Sie in „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“ unter „Sicherheit“ in der Beschreibung zum Blockieren von WAN-Anfragen.

Da Sie das Gateway für den gemeinsamen Zugriff auf Ihre DSL-Internetverbindung verwenden, fragen Sie Ihren ISP, ob Ihrem Konto eine statische IP-Adresse zugewiesen wurde. Ist dies der Fall, benötigen Sie diese statische IP-Adresse für die Konfiguration des Gateways. Sie erhalten diese Informationen von Ihrem ISP.

Dynamische IP-Adressen

Eine dynamische IP-Adresse wird einem Netzwerkgerät, wie z. B. einem Computer oder Druckserver, automatisch zugewiesen. Diese IP-Adressen werden als „dynamisch" bezeichnet, da sie den Netzwerkgeräten nur vorübergehend zugewiesen werden. Nach einem bestimmten Zeitraum laufen Sie ab und können geändert werden. Wenn ein Computer beim Netzwerk (oder im Internet) angemeldet wird und seine dynamische IP-Adresse abgelaufen ist, wird ihm vom DHCP-Server automatisch eine neue dynamische IP-Adresse zugewiesen.

DHCP-Server (*Dynamic Host Configuration Protocol*)

Computern und anderen Netzwerkgeräten mit dynamischen IP-Adressen wird von einem DHCP-Server jeweils eine neue IP-Adresse zugewiesen. Computer bzw. Netzwerkgeräte, die eine IP-Adresse erhalten, werden als DHCP-Clients bezeichnet. Durch DHCP müssen Sie nicht jedes Mal, wenn dem Netzwerk ein neuer Benutzer hinzugefügt wird, manuell eine IP-Adresse zuweisen.

Als DHCP-Server kann entweder ein bestimmter Computer im Netzwerk oder ein anderes Netzwerkgerät, wie z. B. das Gateway, fungieren. Die DHCP-Serverfunktion des Gateways ist standardmäßig aktiviert.

Wenn in Ihrem Netzwerk bereits ein DHCP-Server ausgeführt wird, müssen Sie einen der beiden DHCP-Server deaktivieren. Wenn mehr als ein DHCP-Server in Ihrem Netzwerk ausgeführt werden, treten Netzwerkfehler, wie z. B. IP-Adresskonflikte, auf. Informationen zum Deaktivieren der DHCP-Funktion beim Gateway erhalten Sie in „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways".

Kapitel 3: Beschreibung des Wireless-G ADSL-Home-Gateways

Ports und Reset-Taste an der Seitenwand

Die Ports und die Reset-Taste des Gateways befinden sich an der Seitenwand.

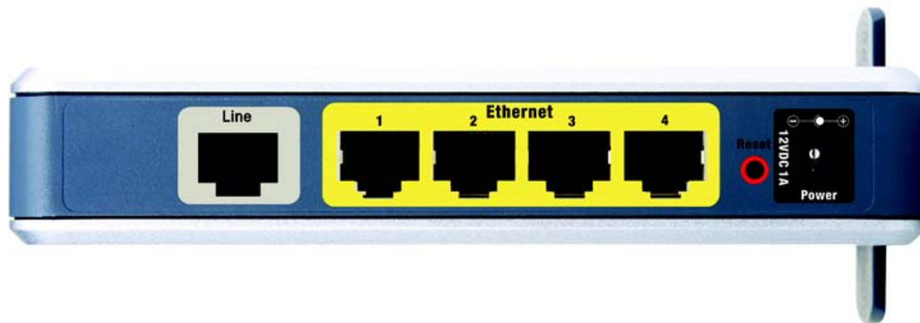


Abbildung 3-1: Ports und Reset-Taste an der Seitenwand

Line (Verbindung) Der **Line**-Port dient zum Anschließen an die ADSL-Verbindung.

Ethernet (1-4) Die **Ethernet**-Ports dienen zum Anschließen an die Computer und andere Netzwerkgeräte.

Reset-Taste Das Gateway kann auf zweierlei Weise auf die Werkseinstellungen zurückgesetzt werden. Halten Sie entweder die **Reset-Taste** ungefähr zehn Sekunden lang gedrückt, oder setzen Sie die Einstellungen im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Administration** (Verwaltung) unter **Factory Defaults** (Werkseinstellungen) zurück.

Power (Netzstrom) Der **Power**-Port dient zum Anschließen des Netzstromadapters.



WICHTIG: Durch das Zurücksetzen des Gateways auf die Werkseinstellungen werden alle Einstellungen gelöscht (einschließlich der Einstellungen für die Internetverbindung, der Wireless-Einstellungen und anderer Einstellungen) und durch die Werkseinstellungen ersetzt. Wenn Sie diese Einstellungen beibehalten möchten, sollten Sie das Gateway nicht zurücksetzen.

LEDs an der Seitenwand

Die LEDs des Gateways, die Netzwerkaktivität anzeigen, befinden sich an der anderen Seitenwand.



Abbildung 3-2: LEDs an der Seitenwand

POWER (Netzstrom) Grün. Die **POWER**-LED leuchtet auf, wenn das Gateway eingeschaltet wird.

WIRELESS Grün. Die **WIRELESS**-LED leuchtet bei jeder erfolgreichen Wireless-Verbindung auf. Wenn die LED blinkt, werden gerade aktiv Daten vom Gateway an eines der Netzwerkgeräte gesendet oder es werden gerade Daten empfangen.

ETHERNET (1-4) Grün. Die **ETHERNET**-LED hat zwei Funktionen. Wenn die LED durchgängig leuchtet, ist das Gateway erfolgreich über den LAN-Port mit einem Gerät verbunden. Wenn die LED blinkt, finden Netzwerkaktivitäten statt.

DSL Grün. Die **DSL-**LED leuchtet bei jeder erfolgreichen DSL-Verbindung auf. Wenn das Gateway eine ADSL-Verbindung herstellt, blinkt die LED.

INTERNET Grün. Die **INTERNET**-LED leuchtet grün auf, wenn eine Internetverbindung zum Internet-Dienstanbieters (ISP) hergestellt wurde. Die **INTERNET**-LED leuchtet rot auf, wenn die Verbindung zum ISP fehlgeschlagen ist.

Untere Gehäusekante

Das Gateway verfügt über einen integrierten Ständer. Wenn Sie das Gateway flach hinlegen möchten, kann der Ständer in geschlossener Position bleiben. Wenn Sie das Gateway jedoch aufrecht hinstellen möchten, drehen Sie den Ständer um 90 º im Uhrzeigersinn und bringen Sie das Gateway in die gewünschte Position.



Abbildung 3-3: Untere Gehäusekante mit Ständer in geschlossener Position



Abbildung 3-4: Gateway mit verwendetem Ständer

Kapitel 4: Anschließen des Wireless-G ADSL-Home-Gateways

Übersicht

In der Regel erhalten Sie vom Installationstechniker Ihres Internet-Dienstanbieters (ISP) nach der Installation der Breitbandverbindung Informationen zur Einrichtung des Modems. Wenn diese Daten nicht zur Verfügung stehen, fordern Sie sie von Ihrem ISP an.

Wenn Sie über die für Ihren Internetverbindungstyp erforderlichen Einrichtungsinformationen verfügen, können Sie mit der Installation und der Einrichtung des Gateways beginnen.

Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Ethernet-Adapter verwenden möchten, fahren Sie mit dem Abschnitt „Verdrahtete Verbindung mit einem Computer" fort. Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Wireless-Adapter verwenden möchten, fahren Sie mit dem Abschnitt „Wireless-Verbindung mit einem Computer" fort.

Verdrahtete Verbindung mit einem Computer

1. Stellen Sie sicher, dass alle Hardwaregeräte des Netzwerks (einschließlich des Gateways und der Computer) ausgeschaltet sind.
2. Schließen Sie ein Ende des Ethernet-Kabels (KAT5) an den Line-Port, der sich an der Rückseite des Gateways befindet, und das andere Ende an den NTPA.



WICHTIG: Benutzer von Annex B (Gateway-Versionen E1 und DE) verwenden zum Anschließen des Gateways an die Wandbuchse (RJ-45 bis RJ-12) das im Lieferumfang enthaltene Spezialkabel. Wenn Sie Splitter oder spezielle Stecker benötigen, wenden Sie sich an Ihren Internet-Dienstanbieter.

3. Schließen Sie ein Ende des Ethernet-Netzwerkkabels an einen der Ethernet-Ports (mit 1-4 beschriftet) an der Seitenwand des Gateways und das andere Ende am Ethernet-Port eines Computers an.

   Wiederholen Sie diesen Schritt, um weitere Computer, einen Switch oder andere Netzwerkgeräte an das Gateway anzuschließen.
4. Schließen Sie den Netzstromadapter an den Netzstrom-Port des Gateways an, und stecken Sie den Netzstromadapter anschließend in eine Steckdose.



HINWEIS: Schließen Sie den Netzstromadapter des Gateways nur an eine Stromleiste mit Überspannungsschutz an.

   Wenn der Netzstromadapter richtig angeschlossen ist, leuchtet die Netzstrom-LED an der Seitenwand grün. Die Netzstrom-LED blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen wurde. Wenn die LED eine Minute oder länger blinkt, finden Sie in „Anhang A: Fehlerbehebung“ entsprechende Informationen.
5. Schalten Sie einen Computer ein, der mit dem Gateway verbunden ist.

Fahren Sie mit „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“ fort.

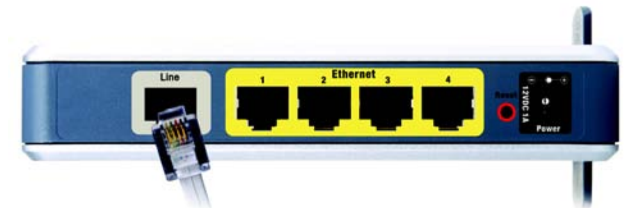


Abbildung 4-1: Herstellen der ADSL-Verbindung



Abbildung 4-2: Anschließen eines PCs

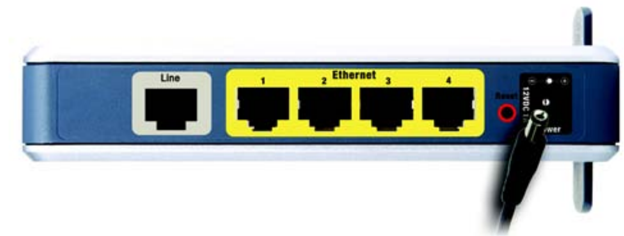


Abbildung 4-3: Anschließen des Netzstroms

Wireless-Verbindung mit einem Computer

Befolgen Sie diese Anweisungen, wenn Sie über eine Wireless-Verbindung auf das Gateway zugreifen möchten:

1. Stellen Sie sicher, dass alle Hardwaregeräte des Netzwerks (einschließlich des Gateways und der Computer) ausgeschaltet sind.
2. Schließen Sie ein Ende des Ethernet-Kabels (KAT5) an den Line-Port auf der Rückseite des Gateways und das andere Ende an den NTPA.



WICHTIG: Benutzer von Annex B (Gateway-Versionen E1 und DE) verwenden zum Anschließen des Gateways an die Wandbuchse (RJ-45 bis RJ-12) das im Lieferumfang enthaltene Spezialkabel. Wenn Sie Splitter oder spezielle Stecker benötigen, wenden Sie sich an Ihren Internet-Dienstanbieter.

3. Schließen Sie den Netzstromadapter an den Netzstrom-Port an, und stecken Sie ihn anschließend in eine Steckdose.

   Wenn der Netzstromadapter richtig angeschlossen ist, leuchtet die Netzstrom-LED an der Seitenwand grün. Die Netzstrom-LED blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen wurde. Wenn die LED eine Minute oder länger blinkt, finden Sie in „Anhang A: Fehlerbehebung“ entsprechende Informationen.

4. Schalten Sie einen der Computer in Ihrem Wireless-Netzwerk ein.
5. Stellen Sie beim erstmaligen Zugriff auf das Gateway über eine Wireless-Verbindung sicher, dass die SSID des Wireless-Adapters des Computers auf **linksys** (die Standardeinstellung des Gateways) eingestellt und die Option zur Sicherheit im Wireless-Netzwerkbetrieb deaktiviert ist. Wenn Sie Zugriff auf das Gateway haben, können Sie die Einstellungen des Gateways und des Adapters dieses Computers an die üblichen Netzwerkeinstellungen anpassen.

Fahren Sie mit „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“ fort.

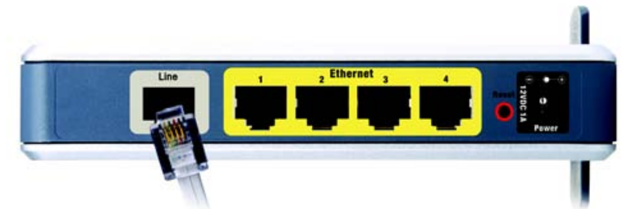


Abbildung 4-4: Herstellen der ADSL-Verbindung



Abbildung 4-5: Anschließen des Netzstroms



HINWEIS: Sie sollten stets die SSID-Standardeinstellung **linksys** ändern und die Option zur Sicherheit im Wireless-Netzwerkbetrieb aktivieren.

Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways

Übersicht

Folgen Sie zum Konfigurieren des Gateways den in diesem Kapitel aufgeführten Schritten, und verwenden Sie das webbasierte Dienstprogramm des Gateways. In diesem Kapitel werden alle Webseiten des Dienstprogramms und deren Hauptfunktionen beschrieben. Sie können das Dienstprogramm mit einem an das Gateway angeschlossenen Computer über Ihren Web-Browser aufrufen. Bei der grundlegenden Netzwerkeinrichtung verwenden die meisten Benutzer die folgenden Fenster des Dienstprogramms:

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie im Fenster **Basic Setup** (Grundlegende Einrichtung) die von Ihrem ISP bereitgestellten Einstellungen ein.
- **Management** (Verwaltungsfunktionen): Klicken Sie auf die Registerkarte **Administration** (Verwaltung) und anschließend auf die Registerkarte **Management** (Verwaltungsfunktionen). Der Standardbenutzername und das Standardpasswort des Gateways lauten **admin**. Ändern Sie das Standardpasswort, um das Gateway zu schützen.

Es gibt sieben Hauptregisterkarten: **Setup** (Einrichtung), **Wireless** (Wireless), **Security** (Sicherheit), **Access Restrictions** (Zugriffsbeschränkungen), **Applications & Gaming** (Anwendungen & Spiele) und **Status** (Status). Wenn Sie auf eine der Hauptregisterkarten klicken, sind jeweils zusätzliche Registerkarten verfügbar.

Setup (Einrichtung)

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie in dieses Fenster die Internetverbindung und die Netzwerkeinstellungen ein.
- **DDNS**: Füllen Sie die Felder dieses Fensters aus, um die Funktion **DDNS** (*Dynamic Domain Name System*) des Gateways zu aktivieren.
- **Advanced Routing** (Erweitertes Routing): In diesem Fenster können Sie die Konfigurationseinstellungen für NAT und Routing ändern.

Wireless

- **Basic Wireless Settings** (Grundlegende Wireless-Einstellungen): In diesem Fenster können Sie die Wireless-Netzwerkeinstellungen auswählen.
- **Wireless Security** (Sicherheit im Wireless-Netzwerkbetrieb): Konfigurieren Sie in diesem Fenster die Wireless-Sicherheitseinstellungen.
- **Wireless Access** (Wireless-Zugriff): In diesem Fenster können Sie den Zugriff auf das Wireless-Netzwerk steuern.
- **Advanced Wireless Settings** (Erweiterte Wireless-Einstellungen): Über dieses Fenster können Sie auf die erweiterten Wireless-Netzwerkeinstellungen zugreifen.



HABEN SIE: TCP/IP auf den Computern aktiviert? Computer tauschen mit diesem Protokoll über das Netzwerk Daten aus. Weitere Informationen zu TCP/IP erhalten Sie in der Windows-Hilfe.



HINWEIS: Für zusätzliche Sicherheit sollten Sie das Passwort über die Registerkarte **Administration** (Verwaltung) ändern.

Security (Sicherheit)

In diesem Fenster können Sie die Firewall deaktivieren bzw. aktivieren, Filter einrichten, WAN-Anfragen blockieren und VPN-Passthrough (*Virtual Private Networks*) aktivieren bzw. deaktivieren.

***VPN** (Virtual Private Network): Sicherheitsmaßnahme, mit der Daten geschützt werden, wenn sie über das Internet von einem Netzwerk in ein anderes übertragen werden.*

Access Restrictions (Zugriffsbeschränkungen)

- **Internet Access** (Internetzugriff): In diesem Fenster können Sie die Internetverwendung und den Datenverkehr im lokalen Netzwerk steuern.

Applications & Gaming (Anwendungen & Spiele)

- **Single Port Forwarding** (Einfaches Port-Forwarding): In diesem Fenster können Sie gängige Dienste oder Anwendungen einrichten, für die das Weiterleiten eines einzelnen Ports erforderlich ist.
- **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich): In diesem Fenster können Sie öffentliche Dienste oder andere spezielle Internetanwendungen einrichten, für die das Weiterleiten eines Anschlussbereichs erforderlich ist.
- **Port Triggering** (Port-Triggering): Klicken Sie auf diese Registerkarte, um die Bereiche für Port-Triggering und Port-Forwarding für Internet-Anwendungen festzulegen.
- **DMZ**: Richten Sie in diesem Fenster die Internetverbindung für einen lokalen Computer so ein, dass spezielle Dienste verwendet werden können.
- **QoS:** Ordnen Sie mit QoS (*Quality of Service*) unterschiedliche Arten der Datenübertragung verschiedenen Prioritätsstufen zu.

Administration (Verwaltung)

- **Management** (Verwaltungsfunktionen): In diesem Fenster können Sie die Einstellungen für den Gateway-Zugriff, für SNMP (*Simple Network Management Protocol*), UPnP (*Universal Plug and Play*), IGMP-Proxy (IGMP ist die Abkürzung für *Internet Group Multicast Protocol*) und für die Wireless-Verwaltung ändern.
- **Reporting** (Berichtaufzeichnung): Klicken Sie auf diese Registerkarte, um Aktivitätsprotokolle anzuzeigen oder zu speichern.
- **Diagnostics** (Diagnose): In diesem Fenster können Sie Ping-Tests ausführen.
- **Backup & Restore** (Sichern & Wiederherstellen): In diesem Fenster können Sie die Konfiguration des Gateways sichern und wiederherstellen.
- **Factory Defaults** (Werkseinstellungen): Verwenden Sie dieses Fenster, wenn Sie die Werkseinstellungen des Gateways wiederherstellen möchten.
- **Firmware Upgrade** (Firmware aktualisieren): Klicken Sie auf diese Registerkarte, um die Gateway-Firmware zu aktualisieren.
- **Reboot** (Neustart): In diesem Fenster können Sie einen Warm- oder Kaltstart des Gateways ausführen.

Status

- **Gateway**: In diesem Fenster sind die Statusinformationen des Gateways aufgeführt.
- **Local Network** (Lokales Netzwerk): In diesem Fenster sind die Statusinformationen des lokalen Netzwerks aufgeführt.
- **Wireless** (Wireless-Netzwerk): In diesem Fenster sind die Statusinformationen des Wireless-Netzwerks aufgeführt.
- **DSL Connection** (DSL-Verbindung): In diesem Fenster sind die Statusinformationen der DSL-Verbindung aufgeführt.

Hinweis für den Zugriff auf das webbasierte Dienstprogramm

Um auf das webbasierte Dienstprogramm zuzugreifen, starten Sie Internet Explorer oder Netscape Navigator und geben Sie im Feld *Adresse* die Standard-IP-Adresse des Gateways (**192.168.1.1**) ein. Drücken Sie anschließend die Eingabetaste.

Daraufhin wird ein Anmeldefenster angezeigt. (Unter Windows XP wird ein ähnliches Fenster angezeigt.) Geben Sie **admin** (als Standardbenutzername) in das Feld *Benutzername* sowie **admin** (als Standardkennwort) in das Feld *Kennwort* ein. Klicken Sie anschließend auf die Schaltfläche **OK**.

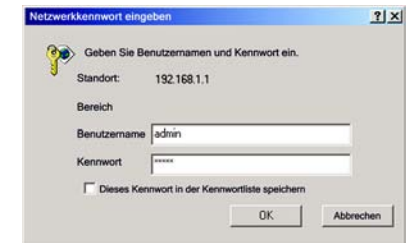


Abbildung 5-1: Anmeldefenster

Registerkarte „Setup“ (Einrichtung)

Registerkarte „Basic Setup“ (Grundlegende Einrichtung)

Im ersten dargestellten Fenster wird die Registerkarte **Basic Setup** (Grundlegende Einrichtung) angezeigt. Auf dieser Registerkarte können Sie die allgemeinen Einstellungen des Gateways ändern. Ändern Sie diese Einstellungen wie hier beschrieben, und klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen zu verwerfen.

Internet-Einrichtung

- **Internet Connection Type** (Internet-Verbindungstyp): Das Gateway unterstützt fünf Kapselungstypen: **RFC 1483 Bridged** (RFC 1483-Überbrückung), **RFC 1483 Routed** (RFC 1483-Weiterleitung), **RFC 2516 PPPoE**, **RFC 2364 PPPoA** und **Bridged Mode Only** (Nur Überbrückungsmodus). Wählen Sie aus dem Dropdown-Menü den geeigneten Kapselungstyp aus. Das jeweilige Fenster *Basic Setup* (Grundlegende Einrichtung) und die verfügbaren Funktionen unterscheiden sich je nach ausgewähltem Kapselungstyp.
- **VC Settings** (VC-Einstellungen): In diesem Bereich können Sie die VC-Einstellungen (*Virtual Circuit*) konfigurieren.
  - **Multiplexing**: Wählen Sie je nach ISP **LLC** (LLC-Multiplexing) oder **VC** (VC-Multiplexing) aus.
  - **QoS Type** (QoS-Typ): Wählen Sie im Dropdown-Menü aus den folgenden Optionen aus: **CBR** (*Continuous Bit Rate;* Konstante Bitrate), um eine feste Bandbreite für Sprach- oder Datenverkehr festzulegen, **UBR** (*Unspecific Bit Rate*; Unbestimmte Bitrate) für Anwendungen, die zeitunabhängig sind (z. B. E-Mail), oder **VBR** (*Variable Bit Rate*; Variable Bitrate) für diskontinuierlichen Verkehr und Bandbreiten, die mit anderen Anwendungen gemeinsam genutzt werden.

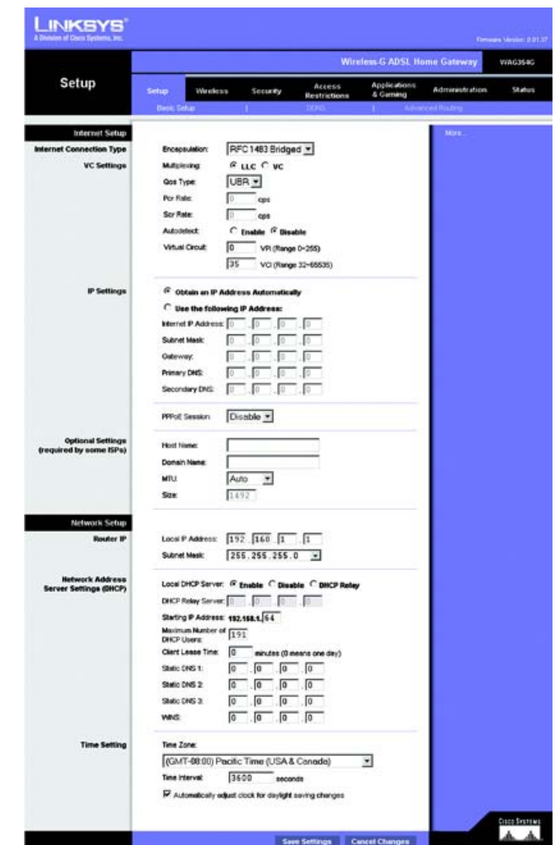


Abbildung 5-2: Grundlegende Einrichtung

- **PCR Rate** (PCR-Rate): Wenn Sie die Rate der DSL-Leitung durch 424 dividieren, erhalten Sie die PCR-Rate, anhand der Sie die maximale Rate, mit der der Absender Zellen senden kann, feststellen können. Geben Sie die Rate in das Feld ein (sofern Ihr Dienstanbieter dies erfordert).

- **SCR Rate** (SCR-Rate): Bestimmt den Mittelwert der Zellrate, die übertragen werden kann. Der Wert der SCR-Rate liegt gewöhnlich unter dem Wert der PCR-Rate. Geben Sie die Rate in das Feld ein (sofern Ihr Dienstanbieter dies erfordert).

- **Autodetect** (Automatisch erkennen): Wählen Sie **Enable** (Aktivieren) aus, damit die Einstellungen automatisch eingegeben werden, oder **Disable** (Deaktivieren), um die Werte manuell einzugeben.

- Virtueller Kreis: Für diese Felder gibt es zwei Optionen: **VPI** (*Virtual Path Identifier*; Virtueller Pfadidentifizierer) und **VCI** (*Virtual Channel Identifier*; Virtueller Kanalidentifizierer). Die korrekten Einstellungen erhalten Sie von Ihrem ISP.

- **IP Settings** (IP-Einstellungen): Befolgen Sie die Anweisungen, die im Abschnitt für den von Ihnen verwendeten Kapselungstyp aufgeführt sind.

RFC 1483-Überbrückung

Dynamische IP-Adresse

IP Settings (IP-Einstellungen): Wählen Sie **Obtain an IP Address Automatically** (IP-Adresse automatisch beziehen), wenn Sie laut Angaben Ihres ISP die Verbindung über eine dynamische IP-Adresse herstellen.

Abbildung 5-3: RFC 1483-Überbrückung - Dynamische IP-Adresse

Statische IP-Adresse

Wenn Sie für die Internetverbindung eine permanente (statische) IP-Adresse verwenden, wählen Sie **Use the following IP Address** (Folgende IP-Adresse verwenden) aus.

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.

- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.

- **Gateway**: Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.

- **Primary DNS** (Primärer DNS; erforderlich) und **Secondary DNS** (Sekundärer DNS; optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

Abbildung 5-4: RFC 1483-Überbrückung - Statische IP-Adresse

RFC 1483-Weiterleitung

Wählen Sie zur Verwendung des Modus **RFC 1483 Routed** (RFC 1483-Weiterleitung) die Option **RFC 1483 Routed** (RFC 1483-Weiterleitung) aus.

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.
- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Gateway**: Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primary DNS** (Primärer DNS; erforderlich) und **Secondary DNS** (Sekundärer DNS; optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

Abbildung 5-5: RFC 1483-Weiterleitung

RFC 2516 PPPoE

Einige ISPs auf DSL-Basis verwenden PPPoE (*Point-to-Point Protocol over Ethernet*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Verbindung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoE verwendet wird. Falls ja, aktivieren Sie die Option **PPPoE**.

- **Service Name** (Dienstname): Geben Sie den Namen Ihres PPPoE-Diensts in dieses Feld ein.
- **User Name** (Benutzername) und **Password** (Passwort): Geben Sie den Benutzernamen und das Passwort ein (von Ihrem ISP bereitgestellt).
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Connect on Demand** (Bei Bedarf verbinden). Geben Sie im Feld *Max Idle Time* (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (Verbindung aufrechterhalten: Wahlwiederholung): Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Keep Alive** (Verbindung aufrechterhalten). Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Standardmäßig erfolgt die Wahlwiederholung nach **20** Sekunden.

Abbildung 5-6: RFC 2516 PPPoE

RFC 2364 PPPoA

Einige ISPs auf DSL-Basis verwenden PPPoA (*Point-to-Point Protocol over ATM*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Leitung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoA verwendet wird. Falls ja, aktivieren Sie die Option **PPPoA**.

- **User Name** (Benutzername) und **Password** (Passwort): Geben Sie den Benutzernamen und das Passwort ein (von Ihrem ISP bereitgestellt).
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Connect on Demand** (Bei Bedarf verbinden). Geben Sie im Feld *Max Idle Time* (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (Verbindung aufrechterhalten: Wahlwiederholung): Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Keep Alive** (Verbindung aufrechterhalten). Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Standardmäßig erfolgt die Wahlwiederholung nach **20** Sekunden.

Abbildung 5-7: RFC 2364 PPPoA

Nur Überbrückungsmodus

Wenn Sie das Gateway als Überbrückung verwenden (dadurch agiert das Gateway als Standalone-Modem), wählen Sie die Option **Bridged Mode Only** (Nur Überbrückungsmodus) aus. In diesem Modus sind alle Einstellungen für NAT und Routing deaktiviert.

Abbildung 5-8: Nur Überbrückungsmodus

Optionale Einstellungen (für einige ISPs erforderlich)

- **Host Name/Domain Name** (Hostname/Domänenname): In diese Felder können Sie einen Hostnamen bzw. Domänennamen für das Gateway eingeben. Für einige ISPs sind diese Namen zu Identifikationszwecken erforderlich. Erfragen Sie bei Ihrem ISP, ob Ihr Breitband-Internetdienst mit einem Host- und Domänennamen konfiguriert wurde. In den meisten Fällen können diese Felder leer gelassen werden.
- **MTU** und **Size** (MTU und Größe): Mit der MTU-Einstellung (*Maximum Transmission Unit*; Maximale Übertragungseinheit) wird die maximale Paketgröße festgelegt, die zur Netzwerkübertragung zugelassen ist. Wählen Sie **Manual** (Manuell) aus, und geben Sie den gewünschten Wert in das Feld *Size* (Größe) ein. Es wird empfohlen, einen Wert zwischen 1200 und 1500 einzugeben. Die maximale Übertragungseinheit (MTU) wird standardmäßig automatisch festgelegt.

Netzwerkeinrichtung

- **Router IP** (IP-Adresse des Routers): Die Werte für die lokale IP-Adresse und Subnetzmaske des Gateways sind hier aufgeführt. In den meisten Fällen können die Standardwerte beibehalten werden.
    - **Local IP Address** (Lokale IP-Adresse): Der Standardwert ist **192.168.1.1**.
    - **Subnet Mask** (Subnetzmaske): Der Standardwert ist **255.255.255.0**.
- **Network Address Server Settings (DHCP)** [Einstellungen des Netzwerkadressenservers (DHCP)]: In diesem Bereich können Sie die DHCP-Einstellungen (*Dynamic Host Configuration Protocol*) des Gateways konfigurieren.
    - **Local DHCP Server** (Lokaler DHCP-Server): Ein DHCP-Server (*Dynamic Host Configuration Protocol*) weist jedem Computer im Netzwerk automatisch eine IP-Adresse zu. Wenn Sie nicht schon über eine IP-Adresse verfügen, ist es äußerst empfehlenswert, das Gateway als DHCP-Server aktiviert zu lassen. Das Gateway kann auch im DHCP-Relay-Modus verwendet werden.
    - **DHCP Relay Server** (DHCP-Relay-Server): Wenn Sie für die Einstellung *Local DHCP Server* (Lokaler DHCP-Server) den DHCP-Relay-Modus aktivieren, geben Sie die IP-Adresse für den DHCP-Server in die entsprechenden Felder ein.
    - **Starting IP Address** (Start-IP-Adresse): Geben Sie einen Wert ein, mit dem der DHCP-Server beim Zuweisen von IP-Adressen beginnen soll. Der Wert muss mindestens 192.168.1.2 betragen, da die Standard-IP-Adresse für das Gateway 192.168.1.1 ist.
    - **Maximum Number of DHCP Users** (Maximale Anzahl der DHCP-Benutzer): Geben Sie die maximale Anzahl von Benutzern bzw. Clients ein, denen eine IP-Adresse zugewiesen werden kann. Diese Zahl hängt von der eingegebenen Start-IP-Adresse ab:
    - **Client Lease Time** (Client-Leasedauer): Bei der Client-Leasedauer handelt es sich um den Zeitraum, in dem ein Computer über seine aktuelle dynamische IP-Adresse eine Verbindung mit dem Gateway herstellen darf. Geben Sie in Minuten an, wie lange diese dynamische IP-Adresse dem Computer zugewiesen bleiben soll.
    - **Static DNS 1-3** (Statisches DNS 1-3): Mit dem DNS (*Domain Name System*) übersetzt das Internet Domänen- oder Website-Namen in Internetadressen oder URLs. Sie erhalten von Ihrem ISP mindestens eine IP-Adresse für den DNS-Server. Hier können Sie bis zu drei IP-Adressen für DNS-Server eingeben. Das Gateway verwendet diese für einen schnelleren Zugriff auf laufende DNS-Server.
    - **WINS**: Mithilfe von WINS (*Windows Internet Naming Service*) werden NetBIOS-Namen in IP-Adressen umgewandelt. Wenn Sie einen WINS-Server verwenden, geben Sie hier die IP-Adresse des Servers ein. Andernfalls lassen Sie dieses Feld leer.
    - **Time Setting** (Zeiteinstellung): Wählen Sie die Zeitzone aus, die sich für den Standort des Gateways eignet. Aktivieren Sie gegebenenfalls das Kontrollkästchen **Automatically adjust clock for daylight saving changes** (Uhr automatisch an Zeitumstellung anpassen).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Abbildung 5-9: Optionale Einstellungen

Registerkarte „DDNS“

Das Gateway verfügt über die Funktion **DDNS** (*Dynamic Domain Name System*). Mit DDNS können Sie einer dynamischen Internet-IP-Adresse einen festen Host- und Domänennamen zuweisen. Dies kann sich für das Hosting Ihrer eigenen Website, Ihres FTP-Servers oder anderer Server hinter dem Gateway als nützlich erweisen.

Bevor Sie diese Funktion verwenden können, müssen Sie sich für den DDNS-Dienst unter www.dyndns.org oder www.tzo.com anmelden.

DDNS

DDNS Service (DDNS-Dienst): Wenn der von Ihnen verwendete DDNS-Dienst von DynDNS.org zur Verfügung gestellt wird, wählen Sie aus dem Dropdown-Menü die Option **DynDNS.org** aus. Wenn der von Ihnen verwendete DDNS-Dienst von TZO.com zur Verfügung gestellt wird, wählen Sie aus dem Dropdown-Menü die Option **TZO.com** aus. Wählen Sie zum Deaktivieren des DDNS-Diensts die Option **Disable** (Deaktivieren) aus.



Abbildung 5-10: DynDNS.org

DynDNS.org

- **User Name** (Benutzername), **Password** (Passwort) und **Host Name** (Hostname): Geben Sie den Benutzernamen, das Passwort und den Hostnamen des mithilfe von DynDNS.org festgelegten Kontos an.
- **Internet IP Address** (Internet-IP-Adresse): Hier ist die aktuelle IP-Adresse des Gateways aufgeführt. Da es sich hierbei um eine dynamische Adresse handelt, kann sie sich ändern.
- **Status**: Hier ist der Status der Verbindung zum DDNS-Dienst aufgeführt.

TZO.com

- **E-mail Address** (E-Mail-Adresse), **Password** (Passwort) und **Domain Name** (Domänenname): Geben Sie die E-Mail-Adresse, das Passwort und den Domänenname des Kontos ein, das Sie bei TZO eingerichtet haben.
- **Internet IP Address** (Internet-IP-Adresse): Hier ist die aktuelle IP-Adresse des Gateways aufgeführt. Da es sich hierbei um eine dynamische Adresse handelt, kann sie sich ändern.
- **Status**: Hier ist der Status der Verbindung zum DDNS-Dienst aufgeführt.



Abbildung 5-11: TZO.com

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Registerkarte „Advanced Routing“ (Erweitertes Routing)

Über das Fenster *Advanced Routing* (Erweitertes Routing) können Sie die Einstellungen für NAT sowie für das dynamische und statische Routing konfigurieren.

Erweitertes Routing

- **Operating Mode** (Betriebsmodus): In diesem Bereich können Sie die allgemeinen Routing-Einstellungen des Gateways konfigurieren.
    - **NAT**: Bei NAT handelt es sich um eine Sicherheitsfunktion, die standardmäßig aktiviert ist. Das Gateway kann dank dieser Funktion IP-Adressen Ihres lokalen Netzwerks in eine andere IP-Adresse für die Internetnutzung umwandeln. Um NAT zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disabled** (Deaktiviert).
    - **RIP:** Wenn Sie mehrere Router einsetzen, empfiehlt es sich, das RIP (*Routing Information Protocol*) zu verwenden, damit die Router untereinander Routing-Informationen austauschen können. Aktivieren Sie zur Verwendung von RIP die Optionsschaltfläche **Enabled** (Aktiviert). Behalten Sie andernfalls die Standardeinstellung **Disabled** (Deaktiviert) bei.
    - **Send Default Route** (Standardroute): Wenn Sie die RIP-Version 1 für das Routing verwenden möchten, aktivieren Sie die Optionsschaltfläche **Enabled** (Aktiviert). Behalten Sie andernfalls die Standardeinstellung **Disabled** (Deaktiviert) bei.
    - **Interface** (Schnittstelle): Diese Einstellung ist dann verfügbar, wenn Sie eine statische Route konfiguriert haben und für diese Route eine Schnittstelle auszuwählen ist. Wählen Sie die vom Gateway zu verwendende Schnittstelle aus: **LAN/Wireless** oder **Internet**.
- **Dynamic Routing** (Dynamisches Routing): Mit der Option **Dynamic Routing** (Dynamisches Routing) kann das Gateway automatisch an physische Änderungen in der Netzwerkanordnung angepasst werden. Bei der Verwendung von RIP legt das Gateway die Route der Netzwerkpakete auf der Grundlage der geringsten Anzahl so genannter Hops (Sprüngen) zwischen Quelle und Ziel fest. Das RIP-Protokoll sendet in regelmäßigen Abständen Routing-Information an andere Gateways im Netzwerk.
    - **Transmit RIP Version** (RIP-Version übertragen): Wählen Sie für die Übertragung von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1**, **RIP1-Compatible** (RIP1-kompatibel) oder **RIP2**: Wenn keine RIP-Nachrichten übertragen werden sollen, wählen Sie **None** (Keine) aus.
    - **Receive RIP Version** (RIP-Version empfangen): Wählen Sie für den Empfang von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1** oder **RIP2**: Wenn keine RIP-Nachrichten empfangen werden sollen, wählen Sie **None** (Keine) aus.

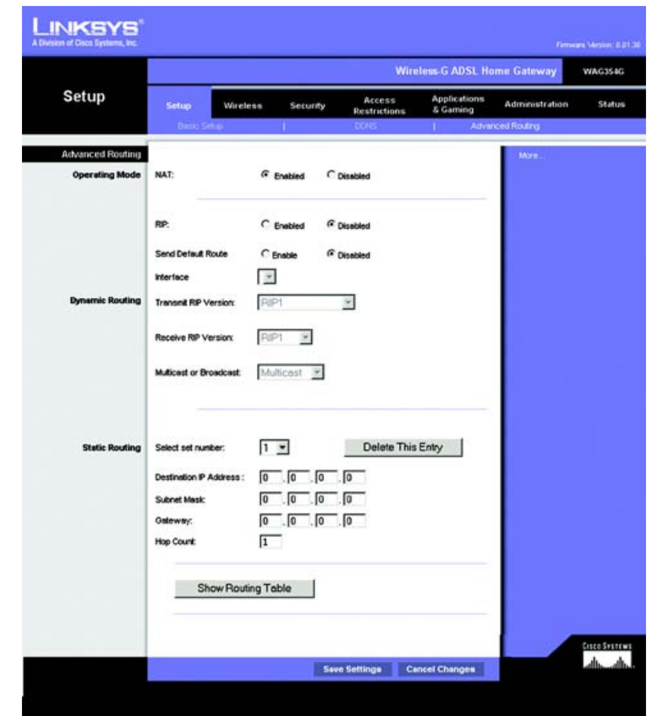


Abbildung 5-12: Erweitertes Routing

- **Multicast** oder **Broadcast**: RIP kann unter Verwendung beider Methoden gesendet werden. Wenn Sie Multicasting verwenden möchten, wählen Sie **Multicast** aus. Wenn Sie Broadcasting verwenden möchten, wählen Sie **Broadcast** aus.

- **Static Routing** (Statisches Routing): Wenn das Gateway mit mehreren Netzwerken verbunden ist, muss zwischen den Netzwerken u. U. eine statische Route eingerichtet werden. Eine statische Route ist ein vordefinierter Pfad, über den Netzwerkinformationen an einen bestimmten Host oder ein bestimmtes Netzwerk übertragen werden. Ändern Sie die folgenden Einstellungen, um eine statische Route zu erstellen:

  - **Select set number** (Set-Nummer auswählen): Wählen Sie die Anzahl der statischen Routen aus dem Dropdown-Menü aus. Das Gateway unterstützt bis zu 20 Einträge für statische Routen. Wenn Sie eine Route löschen möchten, wählen Sie den entsprechenden Eintrag aus und klicken Sie auf die Schaltfläche **Delete This Entry** (Diesen Eintrag löschen).

  - **Destination IP Address** (Ziel-IP-Adresse): Bei der Ziel-IP-Adresse handelt es sich um die Adresse des entfernten Netzwerks bzw. Hosts, dem Sie eine statische Route zuweisen möchten. Geben Sie die IP-Adresse des Hosts ein, für den Sie eine statische Route erstellen möchten. Wenn Sie eine Route zu einem gesamten Netzwerk erstellen, vergewissern Sie sich, dass für den Netzwerkbereich der IP-Adresse der Wert **0** eingestellt ist.

  - **Subnet Mask** (Subnetzmaske): Geben Sie die Subnetzmaske (auch Netzwerkmaske genannt) ein, mit der festgelegt wird, welcher Bereich einer IP-Adresse der Netzwerkbereich und welcher Bereich der Hostbereich ist.

  - **Gateway**: Geben Sie die IP-Adresse des Gateway-Geräts ein, das eine Verbindung zwischen dem Gateway und dem entfernten Netzwerk bzw. Host ermöglicht.

  - **Hop Count** (Anzahl der Gateways): Gibt die Anzahl der Gateways bis zu den einzelnen Knoten an, bevor das Ziel erreicht wird (max. 16 Gateways). Geben Sie diese Zahl in das entsprechende Feld ein.

- **Show Routing Table** (Routing-Tabelle anzeigen): Klicken Sie auf die Schaltfläche **Show Routing Table** (Routing-Tabelle anzeigen), um ein Fenster zu öffnen, in dem die Art der Datenroutings durch Ihr LAN angezeigt wird. Für jede Route wird die IP-Adresse des Ziel-LANs, die Subnetzmaske, das Gateway und die Schnittstelle angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Daten zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum vorherigen Fenster zurückzukehren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Routing Table Entry List Refresh

Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	LAN & Wireless

Close

Abbildung 5-13: Routing-Tabelle

Registerkarte „Wireless“

Registerkarte „Basic Wireless Settings“ (Grundlegende Wireless-Einstellungen)

Mithilfe dieses Fensters können Sie den Wireless-Netzwerkmodus und die Sicherheit im Wireless-Netzwerkbetrieb festlegen.



Abbildung 5-14: Grundlegende Wireless-Einstellungen

Wireless-Netzwerk

- **Wireless Network Mode** (Wireless-Netzwerkmodus): Wenn sich sowohl 802.11g- als auch 802.11b-Geräte in Ihrem Netzwerk befinden, behalten Sie die Standardeinstellung **Mixed** (Gemischt) bei. Wenn Sie ausschließlich 802.11g-Geräte verwenden, wählen Sie **802.11g** aus. Wenn Sie nur 802.11b-Geräte einsetzen, wählen Sie **802.11b** aus. Wenn Sie den Wireless-Netzwerkbetrieb deaktivieren möchten, wählen Sie **Disabled** (Deaktiviert) aus.

- **Wireless Network Name (SSID)** [Wireless-Netzwerkname (SSID)]: Geben Sie in dieses Feld den Namen für Ihr Wireless-Netzwerk ein. Bei der SSID handelt es sich um den Netzwerknamen, der von allen Geräten im Wireless-Netzwerk verwendet wird. Sie muss für alle Geräte im Wireless-Netzwerk identisch sein. Für die maximal 32 Zeichen lange SSID dürfen alle alphanumerischen Zeichen der Tastatur verwendet werden. Es wird zwischen Groß- und Kleinschreibung unterschieden. Sie sollten die standardmäßige SSID (linksys) in einen eindeutigen Namen Ihrer Wahl ändern.

- **Wireless Channel** (Wireless-Kanal): Wählen Sie aus der Liste den Ihren Netzwerkeinstellungen entsprechenden Kanal aus. Eine korrekte Funktion Ihres Wireless-Netzwerks ist nur gewährleistet, wenn die Übertragung für alle Geräte über denselben Kanal erfolgt. Die Wireless-Computer oder -Clients erkennen den Wireless-Kanal des Gateways automatisch.

- **Wireless SSID Broadcast** (Wireless-SSID-Übertragung): Wenn Wireless-Computer oder -Clients im lokalen Netzwerk nach Wireless-Netzwerken suchen, zu denen sie eine Verbindung herstellen können, erkennen sie die vom Gateway übertragene SSID. Wenn die SSID des Gateways übertragen werden soll, behalten Sie die Standardeinstellung **Enable** (Aktivieren) bei. Wenn die SSID des Gateways nicht übertragen werden soll, wählen Sie **Disable** (Deaktivieren) aus.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Registerkarte „Wireless Security“ (Sicherheit im Wireless-Netzwerkbetrieb)

Mit den Wireless-Sicherheitseinstellungen wird die Sicherheit Ihres Wireless-Netzwerks konfiguriert. Das Gateway unterstützt zwei Optionen für die Sicherheit im Wireless-Netzwerkbetrieb: **WPA Pre-Shared Key** (WPA Vorläufiger gemeinsamer Schlüssel) und **WEP** (WPA steht für *Wi-Fi Protected Access*; dies ist ein höherer Sicherheitsstandard als die WEP-Verschlüsselung. WEP ist die Abkürzung für *Wired Equivalent Privacy*.) Im Folgenden erhalten Sie einen Überblick über diese Sicherheitsstandards. Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Gateways erhalten Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb“. Um die Option zur Sicherheit im Wireless-Netzwerkbetrieb zu deaktivieren, wählen Sie im Dropdown-Menü **Security Mode** (Sicherheitsmodus) die Option **Disable** (Deaktivieren) aus.

WPA Pre-Shared Key (WPA Vorläufiger gemeinsamer Schlüssel): Geben Sie einen gemeinsamen WPA-Schlüssel mit einer Länge von 8 bis 32 Zeichen ein. Legen Sie anschließend den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Codierschlüssel auszutauschen sind.



Abbildung 5-15: WPA Vorläufiger gemeinsamer Schlüssel

WEP: WEP ist eine einfache Verschlüsselungsmethode, die nicht so sicher wie WPA ist. Wählen Sie zur Verwendung von WEP einen Wert für **Default Key** (Standardschlüssel; zeigt an, welcher Schlüssel verwendet werden soll) sowie als WEP-Verschlüsselungsebene **64 bits 10 hex digits** (64 Bit 10 Hexadezimalziffern) oder **128 bits 26 hex digits** (128 Bit 26 Hexadezimalziffern) aus. Erstellen Sie anschließend einen WEP-Schlüssel, indem Sie entweder die Passphrase verwenden oder den WEP-Schlüssel manuell eingeben.

- **WEP Encryption** (WEP-Verschlüsselung): WEP ist die Abkürzung für *Wired Equivalent Privacy*. Hierbei handelt es sich um eine Verschlüsselungsmethode zum Schutz der Wireless-Datenkommunikation. WEP basiert auf einem 64-Bit- oder 128-Bit-Schlüssel zur Steuerung des Zugriffs auf Ihr Netzwerk und zur höheren Sicherheit durch Verschlüsselung der Datenübertragung. Um übertragene Daten zu entschlüsseln, müssen alle Geräte im Netzwerk den gleichen WEP-Schlüssel verwenden. Höhere Verschlüsselungsebenen bieten eine höhere Sicherheitsstufe, durch die Komplexität der Verschlüsselung kann jedoch die Netzwerkleistung vermindert werden. Wählen Sie zum Aktivieren von WEP **64 bits 10 hex digits** (64 Bit 10 Hexadezimalziffern) oder **128 bits 26 hex digits** (128 Bit 26 Hexadezimalziffern) aus.

- **Default Transmit Key** (Standard-Übertragungsschlüssel): Legen Sie fest, welcher WEP-Schlüssel (1 bis 4) verwendet werden soll, wenn Daten über das Gateway übertragen werden. Stellen Sie sicher, dass vom Empfangsgerät (Wireless-Computer oder -Client) derselbe Schlüssel verwendet wird.

- **Passphrase**: Sie können anstelle der manuellen Eingabe von WEP-Schlüsseln eine Passphrase eingeben. Mit dieser Passphrase können Sie mindestens einen WEP-Schlüssel erstellen. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden, und die Länge von 32 alphanumerischen Zeichen darf nicht überschritten werden. (Diese Passphrase ist nur mit Wireless-Produkten von Linksys kompatibel und kann nicht mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung verwendet werden. Wenn Sie mit Wireless-Produkten anderer Hersteller oder mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung kommunizieren möchten, notieren Sie sich den im Feld *Key 1* (Schlüssel 1) generierten WEP-Schlüssel und geben Sie ihn manuell in den Wireless-Computer oder -Client ein.) Klicken Sie nach Eingabe der Passphrase auf **Generate** (Generieren), um WEP-Schlüssel zu erstellen.

- **WEP Keys 1-4** (WEP-Schlüssel 1 - 4): Mithilfe von WEP-Schlüsseln können Sie ein Verschlüsselungsschema für Übertragungen im Wireless-Netzwerk erstellen. Wenn Sie keine Passphrase verwenden, geben Sie manuell einen Wertesatz ein. (Lassen Sie keine Schlüsselfelder leer, und geben Sie nicht in alle Schlüsselfelder den Wert **0** ein, da es sich hierbei nicht um gültige Schlüsselwerte handelt.) Wenn Sie die 64-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 10 hexadezimale Zeichen betragen. Wenn Sie die 128-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 26 hexadezimale Zeichen betragen. Gültige hexadezimale Zeichen sind Zahlen von 0 bis 9 und Buchstaben von A bis F.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Gateways erhalten Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb".



Abbildung 5-16: WEP

Registerkarte „Wireless Access“ (Wireless-Zugriff)

Wireless-Netzwerkzugriff

Wireless Network Access (Wireless-Netzwerkzugriff): Wählen Sie **Allow All** (Alle zulassen) aus, wenn allen Computern der Zugriff auf das Wireless-Netzwerk ermöglicht werden soll. Soll der Zugriff eingeschränkt werden, wählen Sie **Restrict Access** (Zugriff beschränken) und anschließend zum Verweigern des Zugriffs für bestimmte Computer **Prevent** (Verweigern) oder zum Gestatten des Zugriffs für bestimmte Computer **Permit only** (Nur Zugriff) aus. Klicken Sie auf die Schaltfläche **Edit MAC Address Access List** (MAC-Adressen-Filterliste bearbeiten). Daraufhin wird das Fenster *Mac Address Filter List* (MAC-Adressen-Filterliste) angezeigt.

Geben Sie die MAC-Adressen der Computer ein, die Sie festlegen möchten. Wenn Sie eine Liste der MAC-Adressen für Wireless-Computer oder -Clients anzeigen möchten, klicken Sie auf die Schaltfläche **Wireless Client MAC List** (MAC-Liste der Wireless-Clients).

Im Fenster *Wireless Client MAC List* (MAC-Liste der Wireless-Clients) werden Computer mit ihrer jeweiligen IP- und MAC-Adresse aufgeführt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), damit die aktuellsten Informationen angezeigt werden. Wenn der MAC-Adressen-Filterliste ein bestimmter Computer hinzugefügt werden soll, aktivieren Sie das Kontrollkästchen **Enable MAC Filter** (MAC-Filter aktivieren) und klicken Sie anschließend auf die Schaltfläche **Update Filter List** (Filterliste aktualisieren). Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Wireless Client MAC List* (MAC-Liste der Wireless-Clients) zurückzukehren.

Klicken Sie im Fenster *Wireless Client MAC List* (MAC-Liste der Wireless-Clients) zum Speichern der Liste auf die Schaltfläche **Save Settings** (Einstellungen speichern) oder auf **Cancel Changes** (Änderungen verwerfen), um Ihre Einträge zu löschen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).



Abbildung 5-17: Wireless-Netzwerkzugriff

MAC Address Filter List

Enter MAC Address Format: xxxxxxxxxxxx/xx:xx:xx:xx:xx:xx

MAC 01:		MAC 11:	
MAC 02:		MAC 12:	
MAC 03:		MAC 13:	
MAC 04:		MAC 14:	
MAC 05:		MAC 15:	
MAC 06:		MAC 16:	
MAC 07:		MAC 17:	
MAC 08:		MAC 18:	
MAC 09:		MAC 19:	
MAC 10:		MAC 20:	

Wireless Client MAC List

Save Settings | Cancel Changes

Abbildung 5-18: MAC-Adressen-Filterliste

Wireless Client MAC List | Refresh

Computer Name	IP Address	MAC Address	Enable MAC Filter

Update Filter List | Close

Abbildung 5-19: MAC-Liste der Wireless-Clients

Registerkarte „Advanced Wireless Settings“ (Erweiterte Wireless-Einstellungen)

Erweitertes Wireless

In diesem Fenster können Sie auf die folgenden erweiterten Wireless-Funktionen zugreifen: Authentifizierungstyp, Gesteuerte Übertragungsrate, Beacon-Intervall, DTIM-Intervall, Fragmentierungsschwelle und RTS-Schwelle.

- **Authentication Type** (Authentifizierungstyp): Standardmäßig ist die Option **Auto** (Automatisch) ausgewählt, mit der sowohl der Authentifizierungstyp **Open System** (Offenes System) als auch **Shared Key** (Freigegebener Schlüssel) verwendet werden kann. Beim Authentifizierungstyp **Open System** (Offenes System) verwenden Absender und Empfänger zur Authentifizierung keinen WEP-Schlüssel, sie können WEP jedoch zur Datenverschlüsselung verwenden. Wenn nur die Open System-Authentifizierung zugelassen werden soll, wählen Sie **Open System** (Offenes System) aus. Beim Authentifizierungstyp **Shared Key** (Freigegebener Schlüssel) verwenden Absender und Empfänger sowohl zur Authentifizierung als auch zur Datenverschlüsselung einen WEP-Schlüssel. Soll nur die Shared Key-Authentifizierung zugelassen werden, wählen Sie **Shared Key** (Freigegebener Schlüssel) aus. Es wird empfohlen, diese Option im Standardmodus **Auto** (Automatisch) zu belassen, da einige Clients nicht für die Option **Shared Key** (Freigegebener Schlüssel) konfiguriert werden können.
- **Control Tx Rates** (Gesteuerte Übertragungsraten): Die Standardübertragungsrate ist auf **Auto** (Automatisch) eingestellt. Diese Rate sollte gemäß der Geschwindigkeit Ihres Wireless-Netzwerks eingestellt werden. Wählen Sie eine der Übertragungsgeschwindigkeiten aus, oder behalten Sie die standardmäßig eingestellte Option **Auto** (Automatisch) bei, wodurch das Gateway automatisch die schnellstmögliche Datenrate verwendet und die Funktion **Auto-Fallback** (Automatisches Fallback) aktiviert wird. Mit der Funktion für automatisches Fallback wird die optimale Verbindungsgeschwindigkeit zwischen dem Gateway und einem Wireless-Client ermittelt.
- **Beacon Interval** (Beacon-Intervall): Der Standardwert ist **100**. Der Wert des Beacon-Intervalls gibt das Sendeintervall des Beacons an. Ein Beacon ist eine Paket, das vom Gateway zur Synchronisierung des Wireless-Netzwerks übertragen wird.
- **DTIM Interval** (DTIM-Intervall): Der Standardwert ist **1**. Mit diesem Wert wird der DTIM-Intervall (*Delivery Traffic Indication Message*) angegeben. Ein DTIM-Feld ist ein Zeitkontrollfeld, das Clients über das nächste Fenster informiert, in dem nach Broadcast- und Multicast-Meldungen gesucht wird. Wenn das Gateway Broadcast- oder Multicast-Meldungen für die zugewiesenen Clients gepuffert hat, sendet es die nächste DTIM mit einem DTIM-Intervallwert. Die zugewiesenen Clients empfangen das Beacon-Signal und sind zum Empfang der Broadcast- und Multicast-Meldungen bereit.
- **Fragmentation Threshold** (Fragmentierungsschwelle): Dieser Wert sollte bei dem Standardwert von **2346** belassen werden. Er gibt die maximale Größe eines Pakets an, bevor die Daten in mehrere Pakete unterteilt werden. Wenn Sie eine hohe Paketfehlerrate wahrnehmen, können Sie die Fragmentierungsschwelle leicht anheben. Wenn die Fragmentierungsschwelle zu niedrig liegt, kann dies zu einer Verringerung der Netzwerkleistung führen. Es wird nur eine geringfügige Änderung dieses Werts empfohlen.
- **RTS Threshold** (RTS-Schwelle): Dieser Wert sollte bei dem Standardwert von **2347** belassen werden. Bei einem schwankenden Datenfluss wird eine nur geringfügige Änderung empfohlen. Wenn ein Netzwerkpaket kleiner als die voreingestellte RTS-Schwellengröße ist, wird der RTS/CTS-Mechanismus nicht aktiviert. Das Gateway sendet RTS-Blöcke (*Request to Send*) an eine bestimmte Empfangsstation und handelt das Senden eines Datenblocks aus. Nach dem Empfang eines RTS-Blocks antwortet die Wireless-Station mit einem CTS-Block (*Clear to Send*), um das Recht, mit der Übertragung zu beginnen, zu bestätigen.



Abbildung 5-20: Erweiterte Wireless-Einstellungen

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Registerkarte „Security“ (Sicherheit)

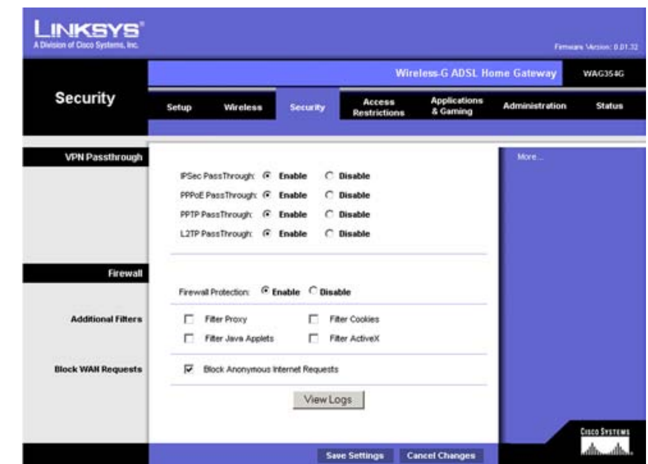


Abbildung 5-21: Sicherheit

In diesem Fenster werden die Einstellungen für VPN-Passthrough, Firewall und Filter angezeigt. Verwenden Sie diese Funktionen, um die Sicherheit des Netzwerks zu erhöhen.

VPN-Passthrough

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, mit der eine sichere Verbindung zwischen zwei entfernten Standorten hergestellt wird. Konfigurieren Sie die folgenden Einstellungen so, dass das Gateway die Übertragung durch VPN-Tunnel zulässt.

- **IPSec Passthrough** (IPSec-Passthrough): IPSec (*Internet Protocol Security*) ist ein Protokollsatz, der zum sicheren Paketaustausch auf der IP-Ebene verwendet wird. Um IPSec-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren). Um IPSec-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disable** (Deaktivieren).
- **PPPoE Passthrough** (PPPoE-Passthrough): Mit PPPoE-Passthrough können Sie die von Ihrem ISP bereitgestellte PPPoE-Client-Software auf Ihren PCs verwenden. Einige ISPs verlangen, dass diese Funktion für das Gateway verwendet wird. Um PPPoE-Passthrough zu aktivieren, klicken Sie auf die Schaltfläche **Enable** (Aktivieren). Um PPPoE-Passthrough zu deaktivieren, klicken Sie auf die Schaltfläche **Disable** (Deaktivieren).
- **PPTP Passthrough** (PPTP-Passthrough): PPTP-Passthrough (*Point-to-Point Tunneling Protocol Passthrough*) ist eine Methode zur Aktivierung von VPN-Sitzungen auf Windows NT 4.0- oder Windows 2000-Servern. Um PPTP-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren). Um PPTP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disable** (Deaktivieren).
- **L2TP Passthrough** (L2TP-Passthrough): Bei L2TP-Passthrough (*Layering 2 Tunneling Protocol Passthrough*) handelt es sich um eine Erweiterung von PPTP (*Point-to-Point Tunneling Protocol*), mit der VPNs über das Internet betrieben werden können. Um P2TP-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren). Um P2TP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disable** (Deaktivieren).

Firewall

Sie können die Firewall aktivieren oder deaktivieren, Filter zum Blockieren bestimmter Internetdatentypen auswählen und anonyme Internet-Anfragen blockieren.

Klicken Sie zum Verwenden der Firewall auf **Enable** (Aktivieren). Wenn die Firewall nicht verwendet werden soll, klicken Sie auf **Disable** (Deaktivieren).

Zusätzliche Filter

- **Filter Proxy** (Filterproxy): Die Verwendung von WAN-Proxyservern kann die Sicherheit des Gateways beeinträchtigen. Wenn Sie den Filterproxy ablehnen, wird der Zugriff auf alle WAN-Proxyserver deaktiviert. Aktivieren Sie zum Verwenden der Proxy-Filterung das entsprechende Kontrollkästchen.
- **Filter Cookies** (Cookies filtern): Bei einem Cookie handelt es sich um Daten, die auf Ihrem Computer gespeichert sind und von Websites beim Zugriff auf diese Sites verwendet werden. Aktivieren Sie zum Verwenden der Cookie-Filterung das entsprechende Kontrollkästchen.
- **Filter Java Applets** (Java-Applets filtern): Bei Java handelt es sich um eine Programmiersprache für Websites. Wenn Sie Java-Applets ablehnen, können Sie u. U. nicht auf Websites zugreifen, die mit dieser Programmiersprache erstellt wurden. Aktivieren Sie zum Verwenden der Java Applet-Filterung das entsprechende Kontrollkästchen.
- **Filter ActiveX** (ActiveX filtern): Bei ActiveX handelt es sich um eine Programmiersprache für Websites. Wenn Sie ActiveX ablehnen, können Sie u. U. nicht auf Websites zugreifen, die mit dieser Programmiersprache erstellt wurden. Aktivieren Sie zum Verwenden der ActiveX-Filterung das entsprechende Kontrollkästchen.

WAN-Anfragen blockieren

- **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren): Mit dieser Option können Sie Ihr Netzwerk vor Ping-Angriffen oder dem Erkennen durch andere Internetbenutzer schützen. Darüber hinaus können Sie mit dieser Option die Sicherheit Ihres Netzwerks erhöhen, indem Ihre Netzwerk-Ports nicht angezeigt werden und Ihr Netzwerk vor Angreifern aus dem Internet besser geschützt ist. Aktivieren Sie die Option **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren), um anonyme Internet-Anfragen zu blockieren bzw. deaktivieren Sie die Option, um anonyme Internet-Anfragen zuzulassen.

Wenn die Aktivitätsprotokolle für die Sicherheitsmaßnahmen angezeigt werden sollen, klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen). Klicken Sie auf die Schaltfläche **Clear** (Löschen), um die Protokollinformationen zu löschen. Klicken Sie auf die Schaltfläche **pageRefresh** (Seite aktualisieren), um die Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Previous Page** (Vorherige Seite), um zur vorherigen Informationsseite zu wechseln. Klicken Sie auf die Schaltfläche **Next Page** (Nächste Seite), um zur nächsten Informationsseite zu wechseln.

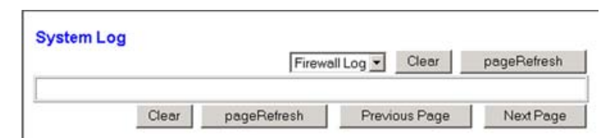


Abbildung 5-22: Firewall-Protokoll

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Registerkarte „Access Restrictions“ (Zugriffsbeschränkungen)

Registerkarte „Internet Access“ (Internetzugriff)

Im Fenster *Internet Access* (Internetzugriff) können Sie bestimmte Arten der Internetverwendung blockieren bzw. zulassen. Sie können für bestimmte Computer Richtlinien für den Internetzugriff einrichten und Websites nach URL-Adresse oder Schlüsselwort blockieren.

Internet Access Policy (Richtlinien für Internetzugriff): Der Zugriff kann mithilfe von Richtlinien verwaltet werden. Mit den Einstellungen in diesem Fenster können Sie Zugriffsrichtlinien erstellen, nachdem Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern) geklickt haben. Wenn Sie aus dem Dropdown-Menü eine Richtlinie ausgewählt haben, werden die Einstellungen dieser Richtlinie angezeigt. Um eine Richtlinie zu löschen, wählen Sie die Nummer dieser Richtlinie aus und klicken Sie auf die Schaltfläche **Delete** (Löschen). Um alle Richtlinien anzuzeigen, klicken Sie auf die Schaltfläche **Summary** (Zusammenfassung). (Sie können Richtlinien aus dem Fenster *Summary* (Zusammenfassung) löschen, indem Sie die entsprechende Richtlinie auswählen und auf die Schaltfläche **Delete** (Löschen) klicken. Um zum Fenster **Internet Access** (Internetzugriff) zurückzukehren, klicken Sie auf die Schaltfläche **Close** (Schließen).)

Status: Die Richtlinien sind standardmäßig deaktiviert. Um eine Richtlinie zu aktivieren, wählen Sie im Dropdown-Menü die Richtlinien-Nummer aus, und aktivieren Sie die Optionsschaltfläche *Enable* (Aktivieren).

So erstellen Sie eine Richtlinie für den Internetzugriff:

1. Wählen Sie im Dropdown-Menü *Internet Access Policy* (Richtlinien für Internetzugriff) eine Nummer aus.
2. Um diese Richtlinie zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren).
3. Geben Sie im Feld **Policy Name** (Richtlinienname) einen Namen für die Richtlinie ein.

Abbildung 5-23: Internetzugriff

Abbildung 5-24: Internet-Richtlinien - Zusammenfassung

4. Klicken Sie auf die Schaltfläche **Edit List of PCs** (Liste der PCs bearbeiten), um die PCs auszuwählen, für die die Richtlinie gelten soll. Das Fenster *List of PCs* (PC-Liste) wird angezeigt. Sie können einen PC nach MAC-Adresse oder IP-Adresse auswählen. Sie können auch mehrere IP-Adressen eingeben, wenn diese Richtlinie für eine Gruppe von PCs gelten soll. Nachdem Sie Ihre Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um Ihre Änderungen anzuwenden, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.
5. Klicken Sie auf die entsprechende Option **Deny** (Verweigern) oder **Allow** (Zulassen), je nachdem, ob Sie den Internetzugriff für die PCs, die Sie im Fenster *List of PCs* (PC-Liste) aufgeführt haben, blockieren oder zulassen möchten.
6. Bestimmen Sie, an welchen Tagen und zu welcher Uhrzeit diese Richtlinie jeweils in Kraft treten soll. Wählen Sie die einzelnen Tage aus, an denen die Richtlinie in Kraft treten soll, oder wählen Sie die Option **Everyday** (Jeden Tag) aus. Geben Sie anschließend die Stunden und Minuten ein, um den Zeitraum festzulegen, in dem die Richtlinie in Kraft treten soll, oder wählen Sie die Option **24 Hours** (24 Stunden) aus.
7. Wenn Sie Websites mit bestimmten URL-Adressen blockieren möchten, geben Sie die entsprechenden URLs in jeweils ein separates Feld neben *Website Blocking by URL Address* (Website nach URL-Adresse blockieren) ein.
8. Wenn Sie Websites mithilfe bestimmter Schlüsselwörter blockieren möchten, geben Sie die entsprechenden Schlüsselwörter in jeweils ein separates Feld neben *Website Blocking by Keyword* (Website nach Schlüsselwort blockieren) ein.
9. Sie können den Zugang zu verschiedenen Diensten filtern, auf die über das Internet, z. B. FTP oder Telnet, zugegriffen werden kann, indem Sie diese Dienste in den Dropdown-Menüs neben *Blocked Services* (Blockierte Dienste) auswählen.

   Geben Sie anschließend den Bereich der Ports ein, den Sie filtern möchten.

   Wenn der Dienst, den Sie blockieren möchten, nicht in der Liste aufgeführt ist, oder wenn Sie die Einstellungen eines Diensts bearbeiten möchten, klicken Sie auf die Schaltfläche **Add/Edit Service** (Dienst hinzufügen/bearbeiten). Daraufhin wird das Fenster *Port Services* (Anschlussdienste) angezeigt.

   Um einen Dienst hinzuzufügen, geben Sie den Namen des Diensts in das Feld *Service Name* (Dienstname) ein. Wählen Sie im Dropdown-Menü *Protocol* (Protokoll) das entsprechende Protokoll aus, und geben Sie den dessen Bereich in die Felder *Port Range* (Anschlussbereich) ein. Klicken Sie anschließend auf die Schaltfläche **Add** (Hinzufügen).

   Um einen Dienst zu bearbeiten, wählen Sie diesen aus der Liste auf der rechten Seite aus. Ändern Sie den Namen, die Protokolleinstellung oder den Anschlussbereich. Klicken Sie anschließend auf die Schaltfläche **Modify** (Bearbeiten).

   Um einen Dienst zu löschen, wählen Sie diesen aus der Liste auf der rechten Seite aus. Klicken Sie anschließend auf die Schaltfläche **Delete** (Löschen).

   Wenn Sie die gewünschten Änderungen im Fenster *Port Services* (Anschlussdienste) vorgenommen haben, klicken Sie auf die Schaltfläche **Apply** (Anwenden), um die Änderungen zu speichern. Wenn Sie Ihre Änderungen verwerfen möchten, klicken Sie auf die Schaltfläche **Cancel** (Abbrechen). Um das Fenster *Port Services* (Anschlussdienste) zu schließen und zum Fenster *Access Restrictions* (Zugriffsbeschränkungen) zurückzukehren, klicken Sie auf die Schaltfläche **Close** (Schließen).
10. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Einstellungen der Richtlinie zu speichern. Um die Einstellungen der Richtlinie rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Abbildung 5-25: PC-Liste

Abbildung 5-26: Dienst hinzufügen/bearbeiten

Registerkarte „Applications and Gaming“ (Anwendungen und Spiele)

Registerkarte „Single Port Forwarding“ (Einfaches Port-Forwarding)

Einfaches Port-Forwarding

Verwenden Sie das Fenster *Single Port Forwarding* (Einfaches Port-Forwarding), wenn ein bestimmter Port geöffnet werden soll, damit Benutzer im Internet die Server hinter dem Gateway erkennen können (zu diesen Servern können FTP- oder E-Mail-Server zählen). Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden PC weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein. Darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

- **Port Map List** (Liste der Port-Zuweisung): In diesem Bereich passen Sie den Port-Dienst an Ihre Anwendungen an.
    - **Application** (Anwendung): Geben Sie den Namen der Anwendung in das entsprechende Feld ein.
    - **External Port** (Externer Port) und **Internal Port** (Interner Port): Geben Sie die Nummern für den externen und internen Port ein.
    - Protocol (Protokoll): Wählen Sie das Protokoll aus, das Sie für die jeweilige Anwendung verwenden möchten: **TCP** oder **UDP**.
    - **IP Address** (IP-Adresse): Geben Sie die IP-Adresse des entsprechenden Computers ein.
    - **Enabled** (Aktiviert): Klicken Sie auf **Enabled** (Aktiviert), um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

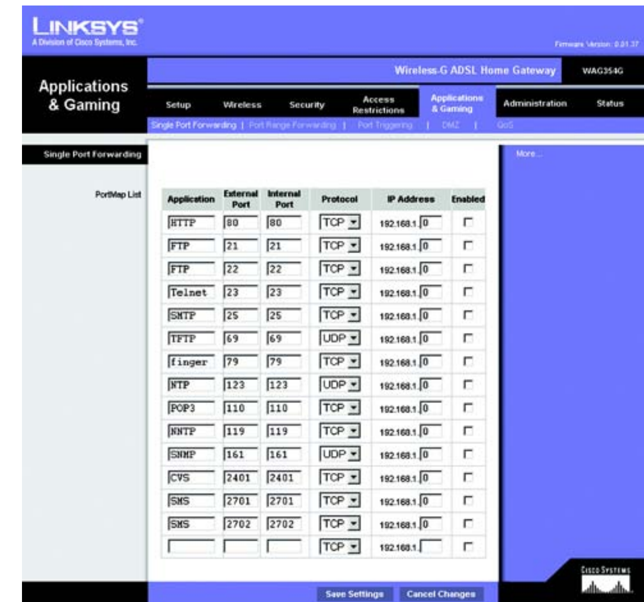


Abbildung 5-27: Einfaches Port-Forwarding

Registerkarte „Port Range Forwarding“ (Weiterleitung an einen Anschlussbereich)

Im Fenster *Port Range Forwarding* (Weiterleitung an einen Anschlussbereich) können Sie öffentliche Dienste auf dem Netzwerk festlegen (z. B. Web-, FTP-, E-Mail-Server oder andere spezielle Internetanwendungen). (Unter speziellen Internetanwendungen versteht man alle Anwendungen, die über den Internetzugang Funktionen wie z. B. Videokonferenzen oder Internet-Spiele ausführen. Bei einigen Internetanwendungen ist keine Weiterleitung erforderlich.)

Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden PC weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein. Darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

- **Application** (Anwendung): Geben Sie den Namen der Anwendung in das entsprechende Feld ein.
- **Start** (Von) und **End** (Bis): Geben Sie die Anfangs- und Endnummern des Anschlussbereichs ein, der weitergeleitet werden soll.
- **Protocol** (Protokoll): Wählen Sie das Protokoll aus, das Sie für die jeweilige Anwendung verwenden möchten: **TCP**, **UDP** oder **Both** (Beide).
- **IP Address** (IP-Adresse): Geben Sie die IP-Adresse des entsprechenden Computers ein.
- **Enable** (Aktivieren): Aktivieren Sie das Kontrollkästchen **Enable** (Aktivieren), um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

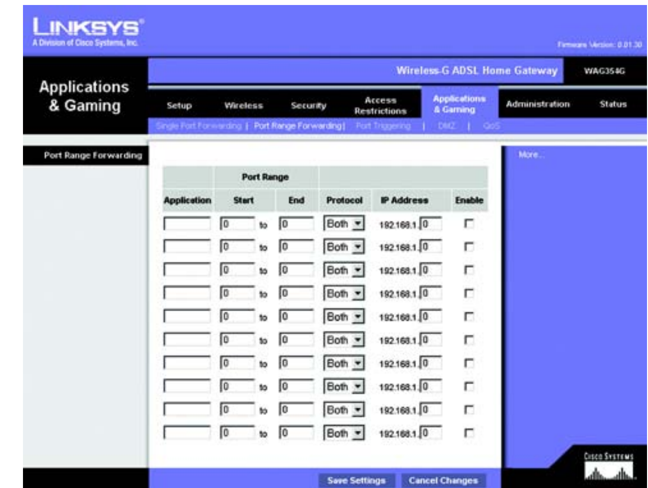


Abbildung 5-28: Port Range Forwarding (Weiterleitung an einen Anschlussbereich)

Registerkarte „Port Triggering“

Port-Triggering wird bei speziellen Anwendungen verwendet, über die ein Anschluss auf Anfrage geöffnet werden kann. Bei dieser Funktion überprüft das Gateway ausgehende Daten auf spezielle Anschlussnummern. Das Gateway speichert die IP-Adresse des Computers, der Daten zur Übertragung abruft. Wenn die abgerufenen Daten über das Gateway übertragen werden, werden die Daten über IP-Adresse und Port-Mapping-Regeln an den entsprechenden Computer weitergeleitet.

- **Application** (Anwendung): Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Triggering Range** (Triggering-Bereich): Geben Sie die Anfangs- und Endnummern der Ports für den Triggering-Bereich ein.
- **Forwarded Range** (Weiterleitungsbereich): Geben Sie die Anfangs- und Endnummern der Ports für den Weiterleitungsbereich ein.
- **Enable** (Aktivieren): Aktivieren Sie das Kontrollkästchen **Enable** (Aktivieren), um das Port-Triggering für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

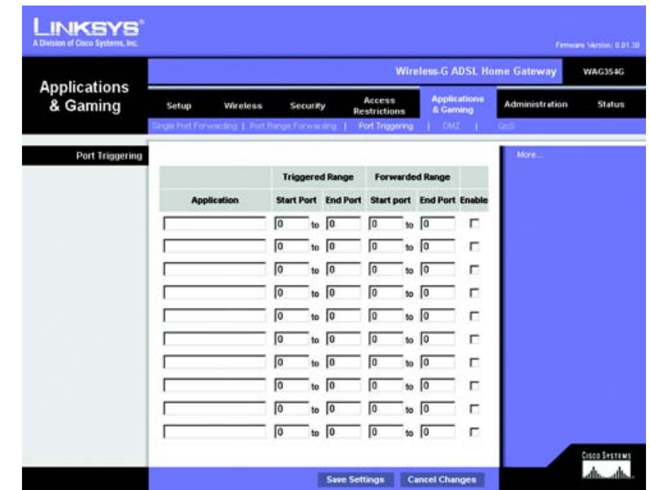


Abbildung 5-29: Port-Triggering

Registerkarte „DMZ“

Über das Fenster *DMZ* kann mithilfe von DMZ-Hosting für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser spezielle Dienste (z. B. Internet-Spiele und Videokonferenzen) nutzen kann. Mit DMZ-Hosting werden alle Ports für einen Computer gleichzeitig weitergeleitet, im Unterschied zu **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich), bei dem nur maximal 10 Anschlussbereiche weitergeleitet werden können.

- **DMZ Hosting** (DMZ-Hosting): Mit der DMZ-Funktion (*Demilitarized Zone*; Entmilitarisierte Zone) kann für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser einen speziellen Dienst, wie z. B. Internet-Spiele oder Videokonferenzen, nutzen kann. Klicken Sie auf **Enable** (Aktivieren), um diese Funktion zu verwenden. Klicken Sie auf **Disable** (Deaktivieren), um die DMZ-Funktion zu deaktivieren.

- **DMZ Host IP Address** (IP-Adresse des DMZ-Hosts): Um einen Computer mit dem Internet zu verbinden, geben Sie die IP-Adresse des Computers ein. Weitere Informationen zum Ermitteln einer IP-Adresse eines Computers finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).



Abbildung 5-30: DMZ

Registerkarte „QoS“

QoS

QoS (*Quality of Service*) sorgt bei Netzwerkverkehr mit hoher Priorität, beispielsweise bei anspruchsvollen Echtzeitanwendungen wie Internettelefonie oder Videokonferenzen, für besseren Service.

Enable/Disable (Aktivieren/Deaktivieren): Wählen Sie zum Verwenden von QoS die Option **Enable** (Aktivieren) aus. Behalten Sie andernfalls die Standardeinstellung **Disable** (Deaktivieren) bei.

Anwendungsbasierte QoS

Über **Application-based QoS** (Anwendungsbasierte QoS) werden Informationen beim Übertragen und Empfangen verwaltet. Je nachdem, welche Einstellungen im Fenster *QoS* festgelegt sind, weist diese Funktion den Informationen von fünf voreingestellten Anwendungen sowie drei zusätzlich angegebenen Anwendungen eine hohe oder niedrige Priorität zu.

High priority/Medium priority/Low priority (Hohe Priorität/Mittlere Priorität/Niedrige Priorität): Wählen Sie für jede der Anwendungen **High priority** (Hohe Priorität; Datenverkehr in dieser Warteschlange belegt 60 % der gesamten Bandbreite), **Medium priority** (Mittlere Priorität; Datenverkehr in dieser Warteschlange belegt 18 % der gesamten Bandbreite) oder **Low priority** (Niedrige Priorität; Datenverkehr in dieser Warteschlange belegt 1 % der gesamten Bandbreite).

FTP (*File Transfer Protocol*): Ein Protokoll für die Übertragung von Dateien über ein TCP/IP-Netzwerk (Internet, UNIX usw.). Nachdem HTML-Seiten für eine Website auf einem lokalen System gestaltet wurden, werden sie üblicherweise über FTP auf den Server geladen.

HTTP (*HyperText Transport Protocol*): Kommunikationsprotokoll, das zum Anschließen von Servern an das World Wide Web verwendet wird. Seine Hauptfunktion besteht darin, eine Verbindung mit einem Webserver herzustellen und HTML-Seiten an den Web-Browser des Clients zu übertragen.

Telnet: Ein Protokoll zur Terminal-Emulation, das häufig in Internet- und TCP/IP-basierten Netzwerken verwendet wird. Dadurch wird Benutzern an Terminals oder Computern ermöglicht, sich bei entfernten Geräten anzumelden und Programme auszuführen.

SMTP (*Simple Mail Transfer Protocol*): **Das standardmäßige E-Mail-Protokoll im Internet.** Ein TCP/IP-Protokoll, mit dem das Meldungsformat sowie der MTA (*Message Transfer Agent*; Meldungsübertragungsagent) festgelegt werden, der die Mail speichert und weiterleitet.

POP3 (*Post Office Protocol 3*): Ein im Internet verbreitet eingesetzter Standard-Mailserver. Er bietet einen Meldungsspeicher, in dem eingehende Mails gespeichert werden, bis sich der entsprechende Empfänger anmeldet und die Mails herunterlädt. POP3 ist ein einfaches System mit wenig Auswahlmöglichkeiten. Alle ausstehenden Meldungen und Anhänge werden zur selben Zeit heruntergeladen. POP3 verwendet das SMTP-Meldungsprotokoll.

Specific Port# (Spezielle Anschlussnummer): Sie können drei weitere Anwendungen hinzufügen, indem Sie deren jeweilige Anschlussnummern in diese Felder eingeben.

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Save Settings** (Einstellungen speichern), oder klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen rückgängig zu machen.

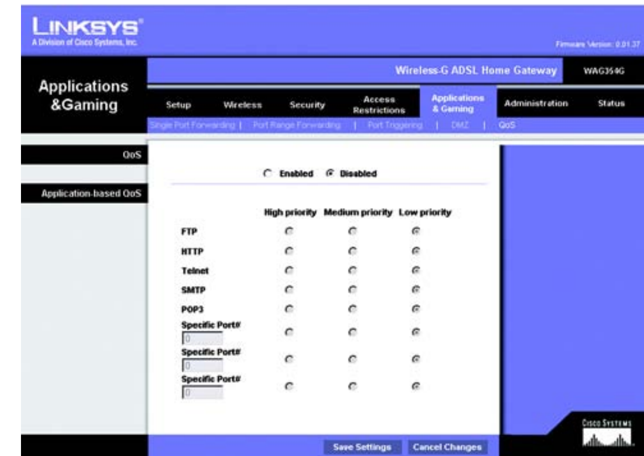


Abbildung 5-31: QoS

Registerkarte „Administration“ (Verwaltung)

Registerkarte „Management“ (Verwaltungsfunktionen)

Über das Fenster *Management* (Verwaltungsfunktionen) können Sie die Einstellungen für den Gateway-Zugriff ändern sowie die Verwaltungsfunktionen für SNMP (*Simple Network Management Protocol*), UPnP (*Universal Plug and Play*), IGMP-Proxy (*Internet Group Multicast Protocol*) und WLAN konfigurieren.

Gateway Access (Gateway-Zugriff)

Local Gateway Access (Lokaler Gateway-Zugriff): Um die Sicherheit des Gateways zu gewährleisten, werden Sie beim Zugriff auf das webbasierte Dienstprogramm des Gateways zur Eingabe Ihres Passworts aufgefordert. Der Standardbenutzername und das Standardpasswort sind **admin**.

- **Gateway Userlist** (Gateway-Benutzerliste): Wählen Sie die Nummer des Benutzers aus dem Dropdown-Menü aus.
- **Gateway Username** (Gateway-Benutzername): Geben Sie den Standardbenutzernamen **admin** ein. Es wird empfohlen, dass Sie Ihren Standardbenutzernamen in einen persönlichen Benutzernamen ändern.
- **Gateway Password** (Gateway-Passwort): Wir empfehlen, das Standardpasswort **admin** in ein Passwort Ihrer Wahl zu ändern.
- **Re-enter to confirm** (Zur Bestätigung erneut eingeben): Geben Sie das neue Gateway-Passwort erneut ein, um es zu bestätigen.

Remote Gatway Access (Entfernter Gateway-Zugriff): Mit dieser Funktion können Sie von einem entfernten Standort aus über das Internet auf das Gateway zugreifen.

- **Remote Management** (Remote-Management): Mit dieser Funktion können Sie das Gateway von einem entfernten Standort aus über das Internet verwalten. Klicken Sie zum Aktivieren von **Remote Management** (Remote-Management) auf **Enable** (Aktivieren).



WICHTIG: Durch Aktivieren der Option **Remote Management** (Remote-Management) kann jeder Benutzer, der Ihr Passwort kennt, von jedem beliebigen Standort im Internet das Gateway konfigurieren.

- **Management Port** (Management-Port): Geben Sie die Anschlussnummer ein, die Sie für den entfernten Zugriff auf das Gateway verwenden möchten.
- **Allowed IP** (Zugelassene IP): Geben Sie die IP-Adressen an, über die das Gateway von einem entfernten Standort aus verwaltet werden kann. Sollen für die IP-Adressen keine Einschränkungen gelten, klicken Sie auf **All** (Alle). Wenn nur eine einzige IP-Adresse angegeben werden soll, klicken Sie auf **IP address** (IP-Adresse) und geben Sie die IP-Adresse in die entsprechenden Felder ein. Um einen IP-Adressen-Bereich anzugeben, wählen Sie **IP range** (IP-Bereich) aus und geben Sie den IP-Adressen-Bereich in die entsprechenden Felder ein.

Remote Upgrade (Remote-Aktualisierung): Mit dieser Funktion kann die Gateway-Firmware von einem entfernten Standort aus über einen TFTP-Server aktualisiert werden. Klicken Sie zum Aktivieren von **Remote Upgrade** (Remote-Aktualisierung) auf **Enable** (Aktivieren).

Abbildung 5-32: Verwaltungsfunktionen

Abbildung 5-33: Zugelassene IP bzw. zugelassener IP-Bereich

SNMP

SNMP ist ein häufig verwendetes Protokoll zur Netzwerküberwachung und -verwaltung. Um **SNMP** zu verwenden, klicken Sie auf **Enabled** (Aktiviert). Um **SNMP** zu deaktivieren, klicken Sie auf **Disabled** (Deaktiviert).

Ist diese Option aktiviert, geben Sie die IP-Adressen ein, denen SNMP-Zugriff gewährt werden soll. Wählen Sie **All** (Alle) aus, wenn für die IP-Adressen keine Einschränkungen gelten sollen, **IP address** (IP-Adresse), wenn Sie eine einzelne IP-Adresse angeben möchten, oder **IP range** (IP-Bereich), wenn Sie einen IP-Adressen-Bereich angeben möchten.

- **Device Name** (Gerätename): Geben Sie den Gateway-Namen ein.
- **SNMP V1/V2**: **Get Community** (Gemeinschaft abrufen): Geben Sie das Passwort ein, mit dem der schreibgeschützte Zugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Set Community** (Gemeinschaft einrichten): Geben Sie das Passwort ein, mit dem der Schreib-/Lesezugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Trap Management**: **Trap to** (Trap-Verwaltung: Trap-Ziel): Geben Sie die IP-Adresse des entfernten Host-Computers ein, der die Trap-Nachrichten erhalten wird.

UPnP

Mit UPnP kann das Gateway unter Windows ME und XP automatisch für verschiedene Internetanwendungen, wie z. B. Internet-Spiele oder Videokonferenzen, konfiguriert werden.

- **UPnP**: Um **UPnP** zu verwenden, klicken Sie auf **Enable** (Aktivieren). Klicken Sie andernfalls auf **Disable** (Deaktivieren).

IGMP-Proxy

Wenn die Multimediaanwendung oder das Gerät hinter dem Gateway nicht ordnungsgemäß funktioniert, können Sie **IGMP-Proxy** aktivieren, um Multicast-Datenverkehr durch das Gateway zuzulassen.

- **IGMP Proxy** (IGMP-Proxy): Klicken Sie auf **Enable** (Aktivieren), um diese Funktion zu verwenden. Andernfalls klicken Sie auf **Disable** (Deaktivieren).

WLAN

- **Management via WLAN** (Verwaltung über WLAN): Mit dieser Funktion kann das Gateway über einen Wireless-Computer des lokalen Netzwerks verwaltet werden, wenn sich dieser beim webbasierten Dienstprogramm des Gateways anmeldet.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Registerkarte „Reporting“ (Berichtaufzeichnung)

Im Fenster *Reporting* (Berichtaufzeichnung) wird ein Protokoll angezeigt, in dem alle eingehenden und ausgehenden URLs bzw. IP-Adressen für die Internetverbindung aufgeführt sind. Über diese Registerkarte stehen auch Protokolle für VPN- und Firewall-Ereignisse zur Verfügung.



Abbildung 5-34: Berichtaufzeichnung

Berichtaufzeichnung

- **Log** (Protokoll): Um die Berichtaufzeichnung zu aktivieren, klicken Sie auf **Enabled** (Aktiviert).
- **Logviewer IP Address** (Logviewer-IP-Adresse): Geben Sie die IP-Adresse des Computers ein, von dem Protokolle empfangen werden. Zum Anzeigen dieser Protokolle ist die Logviewer-Software erforderlich. Diese Software kann kostenlos unter www.linksys.com heruntergeladen werden.

E-Mail-Warnungen

- **Email Alerts** (E-Mail-Warnungen): Um E-Mail-Warnungen zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).
- **Denial of Service Thresholds** (DoS-Schwellenwerte): Geben Sie die Anzahl der DoS-Angriffe (*Denial of Service*) ein, durch die eine E-Mail-Warnung ausgelöst werden soll.
- **SMTP Mail Server** (SMTP Mail-Server): Geben Sie die IP-Adresse des SMTP-Servers ein.
- **E-Mail Address for Alert Logs** (E-Mail-Adresse für Warnungsprotokolle): Geben Sie die E-Mail-Adresse ein, an die Warnungsprotokolle gesendet werden sollen.
- **Return E-Mail address** (E-Mail-Antwortadresse): Geben Sie die Antwortadresse für die E-Mail-Warnungen ein.

Um Protokolle anzuzeigen, klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen). Es wird ein neues Fenster angezeigt. Sie können das anzuzeigende Protokoll aus dem Dropdown-Menü auswählen. Klicken Sie auf die Schaltfläche **Clear** (Löschen), um die Protokollinformationen zu löschen. Klicken Sie auf die Schaltfläche **pageRefresh** (Seite aktualisieren), um die Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Previous Page** (Vorherige Seite), um zur vorherigen Informationsseite zu wechseln. Klicken Sie auf die Schaltfläche **Next Page** (Nächste Seite), um zur nächsten Informationsseite zu wechseln.



Abbildung 5-35: Systemprotokoll

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Registerkarte „Diagnostics“ (Diagnose)

Ping-Test

Ping-Test-Parameter

- **Ping Target IP** (Ping-Ziel-IP-Adresse): Geben Sie die IP-Adresse ein, für die Pings durchgeführt werden sollen. Dies kann eine lokale IP-Adresse (LAN) oder eine Internet-IP-Adresse (WAN) sein.
- **Ping Size** (Ping-Größe): Geben Sie die Größe des Pakets an.
- **Number of Pings** (Anzahl der Pings): Geben Sie an, wie oft die Pings durchgeführt werden sollen.
- **Ping Interval** (Ping-Intervall): Geben Sie den Ping-Intervall (wie oft Pings für die Ziel-IP-Adresse durchgeführt werden sollen) in Millisekunden ein.
- **Ping Timeout** (Ping-Wartezeit): Geben Sie die Ping-Wartezeit (Zeitraum, nach dem der Ping-Test abläuft) in Millisekunden ein.

Klicken Sie auf die Schaltfläche **Start Test** (Test starten), um den Ping-Test zu starten.

- **Ping Result** (Ping-Ergebnisse): In dieser Zeile werden die Ergebnisse des Ping-Tests angezeigt.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).



Abbildung 5-36: Ping-Test

Registerkarte „Backup & Restore“ (Sichern & Wiederherstellen)

Mit der Registerkarte **Backup & Restore** (Sichern & Wiederherstellen) können Sie eine Sicherungskopie der Konfigurationsdatei des Gateways erstellen und diese wiederherstellen.

Konfiguration sichern

Klicken Sie zum Erstellen einer Sicherungskopie der Konfigurationsdatei des Gateways auf die Schaltfläche **Backup** (Sichern). Befolgen Sie dann die Anweisungen auf dem Bildschirm.

Konfiguration wiederherstellen

Klicken Sie zum Wiederherstellen der Konfigurationsdatei des Gateways auf die Schaltfläche **Browse** (Durchsuchen). Befolgen Sie dann die Anweisungen auf dem Bildschirm, um nach der Datei zu suchen. Wenn Sie die Datei gefunden haben, klicken Sie auf die Schaltfläche **Restore** (Wiederherstellen).

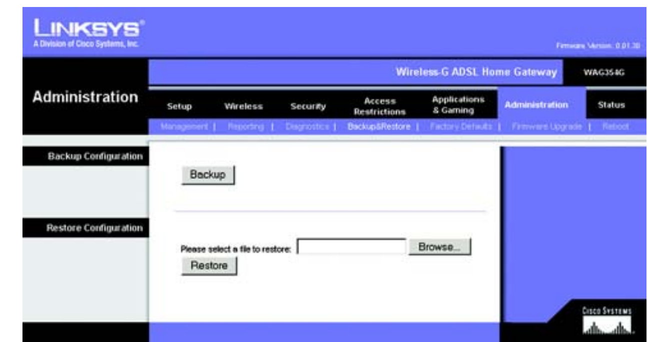


Abbildung 5-37: Sichern & Wiederherstellen

Registerkarte „Factory Defaults“ (Werkseinstellungen)



Abbildung 5-38: Werkseinstellungen

Restore Factory Defaults (Werkseinstellungen wiederherstellen): Wenn Sie das Gateway auf die Werkseinstellungen zurücksetzen möchten (Ihre Einstellungen werden dabei nicht beibehalten), klicken Sie auf **Yes** (Ja).

Um den Wiederherstellungsvorgang zu starten und die Einstellungen zu speichern, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern) bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Registerkarte „Firmware Upgrade“ (Aktualisieren der Firmware)

Mit dem Gateway können Sie Firmware für die LAN-Seite (Netzwerkseite) des Gateways aktualisieren.

Aktualisieren aus dem LAN

So aktualisieren Sie die Gateway-Firmware aus dem LAN:

1. Laden Sie die Datei zum Aktualisieren der Gateway-Firmware unter www.linksys.com/international herunter.
2. Extrahieren Sie die Datei auf Ihrem Computer.
3. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der Firmware-Aktualisierungsdatei zu suchen.
4. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben.
5. Klicken Sie auf die Schaltfläche **Upgrade** (Aktualisieren), und befolgen Sie die Anweisungen auf dem Bildschirm.



Abbildung 5-39: Firmware aktualisieren

Um die Aktualisierung der Firmware abzubrechen, klicken Sie auf die Schaltfläche **Cancel Upgrade** (Aktualisierung abbrechen).

Registerkarte „Reboot“ (Neustart)

In diesem Fenster können Sie einen Warm- oder Kaltstart für das Gateway ausführen. Für die meisten Situationen empfiehlt sich ein Kaltstart. Ein Warmstart ist mit einem Neustart des Computers vergleichbar, bei dem der Computer nicht physisch ausgeschaltet wird.

Neustart

Reboot Mode (Neustart-Modus): Um Ihr Gateway neu zu starten, wählen Sie **Hard** (Kaltstart) oder **Soft** (Warmstart) aus. Um das Gateway aus- und wieder einzuschalten, wählen Sie die Option **Hard** (Kaltstart). Um das Gateway neu zu starten, ohne es auszuschalten, wählen Sie die Option **Soft** (Warmstart) aus.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um den Neustart zu starten. Wenn ein Fenster angezeigt wird, in dem Sie gefragt werden, ob Sie für das Gateway wirklich einen Neustart ausführen möchten, klicken Sie auf **OK**.

Wenn Sie den Neustart abbrechen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).



Abbildung 5-40: Neustart

Registerkarte „Status“

Registerkarte „Gateway“

In diesem Fenster werden Informationen zum Gateway und zu seiner Internetverbindung angezeigt.

Gateway-Informationen

In diesem Bereich wird die Version der Gateway-Firmware, die MAC-Adresse und die aktuelle Uhrzeit angezeigt.

Internetverbindung

In diesem Bereich werden folgende Informationen angezeigt: Verbindung, Anmeldetyp, Schnittstelle, IP-Adresse, Subnetzmaske, Standard-Gateway, IP-Adressen der DNS-Server 1, 2 und 3 sowie die WINS-Adresse.

DHCP Renew (DHCP erneuern): Klicken Sie auf die Schaltfläche **DHCP Renew** (DHCP erneuern), um die aktuelle IP-Adresse des Gateways durch eine neue IP-Adresse zu ersetzen.

DHCP Release (DHCP löschen): Klicken Sie auf die Schaltfläche **DHCP Release** (DHCP löschen), um die aktuelle IP-Adresse des Gateways zu löschen.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.



Abbildung 5-41: Gateway

Registerkarte „Local Network“ (Lokales Netzwerk)

Im Bereich **Local Network** (Lokales Netzwerk) sind Angaben zur lokalen MAC-Adresse, IP-Adresse, Subnetzmaske, zum DHCP-Server sowie zur Start- und End-IP-Adresse aufgeführt. Um die DHCP-Client-Tabelle anzuzeigen, klicken Sie auf die Schaltfläche **DHCP Clients Table** (DHCP-Client-Tabelle). Klicken Sie zum Anzeigen der ARP/RARP-Tabelle auf die Schaltfläche **ARP/RARP Table** (ARP/RARP-Tabelle).

DHCP Client Table (DHCP-Client-Tabelle): Im Bereich **DHCP Active IP Table** (DHCP - Tabelle zur aktiven IP-Adresse) werden die aktuellen DHCP-Client-Daten angezeigt. Zu diesen Angaben zählen der Computername, die IP-Adresse, die MAC-Adresse und der Zeitpunkt, zu dem die dynamische IP-Adresse für die Wireless-Clients, die den DHCP-Server nutzen, abläuft. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Um einen Client vom DHCP-Server zu löschen, wählen Sie den entsprechenden Client aus und klicken Sie anschließend auf die Schaltfläche **Delete** (Löschen). Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Local Network* (Lokales Netzwerk) zurückzukehren.

ARP/RARP Table (ARP/RARP-Tabelle): Im Bereich **ARP/RARP Table** (ARP/RARP-Tabelle) sind die aktuellen Angaben für die Clients des lokalen Netzwerks aufgeführt, die eine ARP-Anfrage an das Gateway gesendet haben. Es werden die entsprechenden IP-Adressen und MAC-Adressen aufgeführt. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Bei einer ARP-Anfrage handelt es sich um eine Anfrage, mit der das Gateway die MAC-Adressen von Clients mit IP-Adressen anfragt, um IP-Adressen den entsprechenden MAC-Adressen zuordnen zu können. Bei RARP geht der Vorgang im Vergleich zu ARP umgekehrt vonstatten. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Local Network* (Lokales Netzwerk) zurückzukehren.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.



Abbildung 5-42: Lokales Netzwerk

DHCP Active IP Table

DHCP Server IP Address: 192.168.1.1

Client Host Name	IP Address	MAC Address	Expires
None	None	None	None

Refresh Delete Close

Abbildung 5-43: DHCP - Tabelle zur aktiven IP-Adresse

ARP/RARP Table

IP Address	MAC Address
192.168.1.64	00:D0:B7:B6:46:BA

Close Refresh

Abbildung 5-44: ARP/RARP-Tabelle

Registerkarte „Wireless“

Im Bereich der Wireless-Netzwerkinformationen sind Angaben zu Wireless-Firmware-Version, MAC-Adresse, Modus, SSID, DHCP-Server, Kanal sowie zur Verschlüsselungsfunktion aufgeführt.

Klicken Sie auf die Schaltfläche **Wireless Clients Connected** (Angeschlossene Wireless-Clients), um eine Liste der Wireless-Clients anzuzeigen, die an das Gateway angeschlossen sind. Gleichzeitig werden die entsprechenden Computernamen, IP-Adressen und MAC-Adressen angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Wireless* zurückzukehren.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.



Abbildung 5-45: Wireless



Abbildung 5-46: Netzwerk-Computer

Registerkarte „DSL Connection“ (DSL-Verbindung)

In diesem Fenster werden Informationen zur DSL- und PVC-Verbindung angezeigt.

DSL-Status

In diesem Bereich werden folgende Informationen angezeigt: DSL-Status, DSL-Modulationsmodus, DSL-Pfadmodus, Downstream-Rate, Upstream-Rate, Downstream-Grenze, Upstream-Grenze, Downstream-Verbindungsabschwächung, Upstream-Verbindungsabschwächung, Downstream-Übertragungsleistung und Upstream-Übertragungsleistung.

PVC-Verbindung

In diesem Bereich werden folgende Informationen angezeigt: Kapselungsmethode, Multiplexing, QoS, PCR-Rate, SCR-Rate, Automatisch erkennen, VPI, VCI, Aktiviert-Status und PVC-Status.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.



Abbildung 5-47: DSL-Verbindung

Anhang A: Fehlerbehebung

Dieser Anhang besteht aus zwei Teilen: „Behebung häufig auftretender Probleme“ und „Häufig gestellte Fragen“. Er enthält Lösungsvorschläge zu Problemen, die während der Installation und des Betriebs des Gateways auftreten können. Lesen Sie sich zur Fehlerbehebung die unten aufgeführten Beschreibungen durch. Wenn hier kein Lösungsvorschlag zu Ihrem Problem aufgeführt ist, finden Sie weitere Informationen auf der Website von Linksys unter www.linksys.com/international.

Behebung häufig auftretender Probleme

1. ***Wie lege ich eine statische IP-Adresse auf einem Computer fest?***
   Führen Sie die folgenden Schritte aus, um einem Computer eine statische IP-Adresse zuzuweisen:
   - Für Benutzer von Windows 98 und ME:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf die Option **Netzwerk**.
     2. Wählen Sie im Feld **Die folgenden Netzwerkkomponenten sind installiert** die mit dem Ethernet-Adapter verbundene Option **TCP/IP->** aus. Falls nur ein Ethernet-Adapter installiert ist, wird nur in einer Zeile „TCP/IP“ ohne Verknüpfung mit einem Ethernet-Adapter aufgeführt. Wählen Sie den Eintrag aus, und klicken Sie auf die Schaltfläche **Eigenschaften**.
     3. Wählen Sie im Fenster für die TCP/IP-Eigenschaften in der Registerkarte **IP-Adresse** die Option **IP-Adresse festlegen** aus. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird. Vergewissern Sie sich, dass für jeden Computer bzw. jedes Netzwerkgerät eine eindeutige IP-Adresse verwendet wird.
     4. Klicken Sie auf die Registerkarte **Gateway** und geben Sie 192.168.1.1 ein, wenn die Eingabeaufforderung für das neue Gateway angezeigt wird (dies ist die Standard-IP-Adresse für das Gateway). Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Eingabe zu übernehmen.
     5. Klicken Sie auf die Registerkarte **DNS**, und stellen Sie sicher, dass die Option **DNS** aktiviert ist. Geben Sie den Host- und den Domänennamen ein (z. B. „Johann“ als Hostname und „home“ als Domänenname). Geben Sie den DNS-Eintrag ein, den Sie von Ihrem ISP erhalten haben. Falls Sie keine DNS-IP-Adresse von Ihrem ISP erhalten haben, wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
     6. Klicken Sie im Fenster für die TCP/IP-Eigenschaften auf **OK**, und klicken Sie anschließend auf die Schaltfläche **Schließen** bzw. die Schaltfläche **OK**, um das Fenster **Netzwerk** zu schließen.
     7. Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.
   - Für Benutzer von Windows 2000:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Netzwerk- und DFÜ-Verbindungen**.

2. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
3. Wählen Sie im Feld **Aktivierte Komponenten werden von dieser Verbindung verwendet** die Option **Internetprotokoll (TCP/IP)** aus, und klicken Sie auf die Schaltfläche **Eigenschaften**. Wählen Sie die Option **Folgende IP-Adresse verwenden** aus.
4. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
5. Geben Sie für die Subnetzmaske den Eintrag 255.255.255.0 ein.
6. Geben Sie für das Standardgateway den Eintrag 192.168.1.1 ein (die Standard-IP-Adresse des Gateways).
7. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
8. Klicken Sie im Fenster **Internetprotokolleigenschaften (TCP/IP)** auf die Schaltfläche **OK** sowie im Fenster **Eigenschaften von LAN-Verbindung** auf die Schaltfläche **OK**.
9. Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.

- Für Benutzer von Windows XP:
  Die folgenden Anweisungen gelten, wenn Sie Windows XP mit der Standard-Benutzeroberfläche ausführen. Wenn Sie die klassische Benutzeroberfläche verwenden (bei der die Symbole und Menüs wie in vorherigen Windows-Versionen aussehen), befolgen Sie die Anweisungen für Windows 2000.

1. Klicken Sie auf **Start** und **Systemsteuerung**.
2. Klicken Sie auf das Symbol **Netzwerk- und Internetverbindungen** und dann auf **Netzwerkverbindungen**.
3. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
4. Wählen Sie im Feld **Diese Verbindung verwendet folgende Elemente** die Option **Internetprotokoll (TCP/IP)**. Klicken Sie auf die Schaltfläche **Eigenschaften**.
5. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
6. Geben Sie für die Subnetzmaske den Eintrag 255.255.255.0 ein.
7. Geben Sie für das Standardgateway den Eintrag 192.168.1.1 ein (die Standard-IP-Adresse des Gateways).
8. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
9. Klicken Sie im Fenster **Internetprotokolleigenschaften (TCP/IP)** auf die Schaltfläche **OK**. Klicken Sie im Fenster **Eigenschaften von LAN-Verbindung** auf die Schaltfläche **OK**.

2. Ich möchte meine Internetverbindung prüfen.

A. Überprüfen Sie Ihre TCP/IP-Einstellungen.

Für Benutzer von Windows 98, ME, 2000 und XP:

- Weitere Informationen finden Sie in der Windows-Hilfe. Stellen Sie sicher, dass in den Einstellungen die Option **IP-Adresse automatisch beziehen** aktiviert ist.

Für Benutzer von Windows NT 4.0:

- Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf das Symbol **Netzwerk**.
- Klicken Sie auf die Registerkarte **Protokoll**, und doppelklicken Sie auf **TCP/IP-Protokoll**.
- Wenn das Fenster angezeigt wird, stellen Sie sicher, dass Sie den richtigen Adapter als Ihren Ethernet-Adapter und die Option **IP-Adresse von einem DHCP-Server beziehen** ausgewählt haben.
- Klicken Sie im Fenster mit den TCP/IP-Protokolleigenschaften auf die Schaltfläche **OK** und im Fenster **Netzwerk** auf die Schaltfläche **Schließen**.
- Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.

B. Öffnen Sie eine Eingabeaufforderung.

Für Benutzer von Windows 98 und ME:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie in das Feld **Öffnen** den Eintrag **command** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

Für Benutzer von Windows NT, 2000 und XP:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen** den Eintrag **cmd** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**. Geben Sie in die Eingabeaufforderung den Eintrag **ping 192.168.1.1** ein, und drücken Sie die Eingabetaste.
- Wenn Sie eine Antwort erhalten, kommuniziert der Computer mit dem Gateway.
- Wenn Sie KEINE Antwort erhalten, überprüfen Sie die Kabelverbindung und stellen Sie sicher, dass in den TCP/IP-Einstellungen für den Ethernet-Adapter die Option **IP-Adresse automatisch beziehen** aktiviert ist.

C. Geben Sie in die Eingabeaufforderung den Eintrag **ping** gefolgt von Ihrer Internet- bzw. WAN-IP-Adresse ein, und drücken Sie die Eingabetaste. Die Internet- bzw. WAN-IP-Adresse wird im Statusfenster des webbasierten Dienstprogramms des Gateways angezeigt. Beispiel: Wenn Ihre Internet- bzw. WAN-IP-Adresse 1.2.3.4 lautet, müssen Sie den Eintrag **ping 1.2.3.4** eingeben und anschließend die Eingabetaste drücken.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Gateway verbunden.
- Wenn Sie KEINE Antwort erhalten, geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

D. Geben Sie in die Eingabeaufforderung den Eintrag **ping www.yahoo.com** ein, und drücken Sie die Eingabetaste.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Internet verbunden. Wenn Sie KEINE Website öffnen können, geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.
- Wenn Sie KEINE Antwort erhalten, kann ein Verbindungsproblem vorliegen. Geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

3. Mit meiner Internetverbindung erhalte ich keine IP-Adresse im Internet.

- Lesen Sie sich den oben aufgeführten Abschnitt „2. Ich möchte meine Internetverbindung prüfen“ durch, und überprüfen Sie anhand dessen Ihre Verbindung.
  1. Stellen Sie sicher, dass Sie die korrekten Einstellungen für die Internetverbindung verwenden. Wenden Sie sich an Ihren ISP, um die Art Ihrer Internetverbindung zu überprüfen: RFC 1483 Bridged (RFC 1483-Überbrückung), RFC 1483 Routed (RFC 1483-Übertragung), RFC 2516 PPPoE oder RFC 2364 PPPoA. Weitere Einzelheiten zu den Einstellungen für die Internetverbindung finden Sie in „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“ im Abschnitt zur Registerkarte **Setup** (Einrichten).
  2. Stellen Sie sicher, dass Sie das richtige Kabel verwenden. Überprüfen Sie, ob in der Spalte für das Gateway die ADSL-LED konstant leuchtet.
  3. Stellen Sie sicher, dass das an den ADSL-Port Ihres Gateways angeschlossene Kabel in die Wandbuchse der ADSL-Verbindung eingesteckt ist. Überprüfen Sie, ob in der Statusseite des webbasierten Dienstprogramms des Gateways eine gültige IP-Adresse Ihres ISP aufgeführt ist.
  4. Schalten Sie den Computer und das Gateway aus. Warten Sie 30 Sekunden, und schalten Sie dann das Gateway und den Computer wieder ein. Überprüfen Sie, ob im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Status** eine IP-Adresse angezeigt wird.

4. Ich kann auf die Setup-Seite des webbasierten Dienstprogramms des Gateways nicht zugreifen.

- Informationen zur Überprüfung einer ordnungsgemäßen Verbindung des Computers mit dem Gateway finden Sie unter „2. Ich möchte meine Internetverbindung prüfen“.
  1. Informationen zur Überprüfung, ob Ihr Computer eine IP-Adresse, eine Subnetzmaske, ein Gateway und einen DNS besitzt, finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
  2. Legen Sie eine statische IP-Adresse für Ihren Computer fest. Weitere Informationen hierzu finden Sie unter „1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?“.
  3. Folgen Sie den Anweisungen unter „10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?

5. Mein VPN (Virtual Private Network) funktioniert nicht über das Gateway.

Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf, und öffnen Sie die Registerkarte **Security** (Sicherheit). Stellen Sie sicher, dass Sie die Option **IPSec Passthrough** (IPSec-Passthrough) und/oder **PPTP Passthrough** (PPTP-Passthrough) aktiviert haben.

- VPNs, in denen IPSec mit der ESP-Authentifizierung (*Encapsulation Security Payload*, auch als Protokoll 50 bezeichnet) verwendet wird, funktionieren einwandfrei. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen. Je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.
- VPNs, in denen IPSec und AH (*Authentication Header*, auch als Protokoll 51 bezeichnet) verwendet werden, sind mit dem Gateway nicht kompatibel. Die Verwendung von AH ist aufgrund gelegentlicher Inkompatibilität mit dem NAT-Standard beschränkt.

- Ändern Sie die IP-Adresse des Gateways auf ein anderes Subnetz, so dass Konflikte zwischen der IP-Adresse des VPNs und Ihrer lokalen IP-Adresse vermieden werden. Wenn Ihr VPN-Server beispielsweise die IP-Adresse 192.168.1.X zuweist (wobei „X" für eine Zahl zwischen 1 und 254 steht) und die IP-Adresse Ihres LANs 192.168.1.X lautet (wobei „X" mit der in der IP-Adresse des VPNs verwendeten Zahl identisch ist), werden Informationen vom Gateway u. U. nicht richtig übertragen. Zur Problembehebung ändern Sie die IP-Adresse des Gateways in 192.168.2.1. Ändern Sie die IP-Adresse des Gateways im webbasierten Dienstprogramm auf der Registerkarte **Setup** (Einrichtung).
- Wenn Sie einem Computer oder einem anderen Gerät in Ihrem Netzwerk eine statische IP-Adresse zugewiesen haben, müssen Sie seine IP-Adresse dementsprechend in 192.168.2.Y (wobei „Y" für eine Zahl zwischen 1 und 254 steht) ändern. Beachten Sie, dass jede IP-Adresse im Netzwerk eindeutig sein muss.
- Bei Ihrem VPN ist es u. U. erforderlich, dass Port 500/UDP-Pakete an den Computer übertragen werden, der mit dem IPSec-Server verbunden ist. Details hierzu finden Sie unter „7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internet-Anwendungen verwenden."
- Weitere Informationen finden Sie auf der Website von Linksys unter www.linksys.com/international.

6. Wie richte ich einen Server hinter dem Gateway ein und gebe ihn für alle Benutzer frei?

Um einen Server als Web-, FTP- oder Mail-Server zu verwenden, muss Ihnen die jeweils verwendete Anschlussnummer bekannt sein. Beispiel: Port 80 (HTTP) wird für Webserver, Port 21 (FTP) für FTP-Server und Port 25 (SMTP Ausgang) sowie Port 110 (POP3 Eingang) für Mail-Server verwendet. Weitere Informationen finden Sie in der Dokumentation des installierten Servers.

- Befolgen Sie die hier aufgeführten Schritte, um die Port-Weiterleitung über das webbasierte Dienstprogramm des Gateways einzurichten. Im Folgenden finden Sie Anweisungen zum Einrichten von Web-, FTP- und Mail-Servern.
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
  2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
  3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Wenn Sie beispielsweise einen Webserver verwenden, legen Sie den Bereich zwischen 80 und 80 fest.
  4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
  5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert 100 in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters".

6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Aktivieren**. Beachten Sie folgendes Beispiel:

Benutzerdefinierte Anwendung	Externer Anschluss	TCP	UDP	IP-Adresse	Aktivieren
Webserver	80 bis 80	X		192.168.1.100	X
FTP-Server	21 bis 21	X		192.168.1.101	X
SMTP (Ausgang)	25 bis 25	X		192.168.1.102	X
POP3 (Eingang)	110 bis 110	X		192.168.1.102	X

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internetanwendungen verwenden.

Zum Verwenden von Online-Spielen oder Internetanwendungen ist i. d. R. keine Port-Weiterleitung bzw. kein DMZ-Hosting notwendig. In einigen Fällen müssen Sie u. U. das Hosting für Online-Spiele oder Internetanwendungen anwenden. Dafür müssen Sie das Gateway so einrichten, dass eingehende Datenpakete oder Daten an einen bestimmten Computer geliefert werden. Dies trifft auch auf die verwendeten Internetanwendungen zu. Sie erhalten Informationen zu den zu verwendenden Anschlussdiensten auf der Website des betreffenden Online-Spiels bzw. der Anwendung, das bzw. die Sie verwenden möchten. Führen Sie diese Schritte aus, um ein Hosting für ein Online-Spiel auszuführen bzw. um eine bestimmte Internetanwendung zu verwenden:

1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Um beispielsweise Unreal Tournament (UT) auszuführen, müssen Sie den Bereich von 7777 bis 27900 eingeben.
4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert 100 in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Aktivieren**. Beachten Sie folgendes Beispiel:

Benutzerdefinierte Anwendung	Externer Anschluss	TCP	UDP	IP-Adresse	Aktivieren
UT	7777 bis 27900	X	X	192.168.1.100	X
Halflife	27015 bis 27015	X	X	192.168.1.105	X
PCAnywhere	5631 bis 5631		X	192.168.1.102	X
VPN/IPSEC	500 bis 500		X	192.168.1.100	X

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

8. ***Weder Internetspiele, Internetserver noch Internetanwendungen funktionieren.***
   Falls Sie Schwierigkeiten haben, Internetspiele, -server und -anwendungen zu verwenden, verbinden Sie einen Computer über das DMZ-Hosting (*DeMilitarized Zone*) mit dem Internet. Diese Option ist verfügbar, wenn für eine Anwendung zu viele Ports erforderlich sind oder Sie nicht sicher sind, welchen Anschlussdienst Sie verwenden sollen. Stellen Sie sicher, dass alle Weiterleitungseinträge deaktiviert sind, um das DMZ-Hosting erfolgreich zu verwenden, da das Forwarding Vorrang vor dem DMZ-Hosting hat. (Mit anderen Worten: In dem Gateway eingehende Daten werden zuerst hinsichtlich ihrer Forwarding-Einstellungen überprüft. Falls die Daten von einer Portnummer eingehen, für die keine Port-Weiterleitung aktiviert ist, sendet das Gateway die Daten an einen beliebigen Computer oder ein beliebiges Netzwerkgerät, der bzw. das für DMZ-Hosting festgelegt wurde.)
   - Führen Sie folgende Schritte aus, um DMZ-Hosting festzulegen:
     1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **DMZ** auf. Wählen Sie **Enabled** (Aktiviert) aus, und geben Sie die IP-Adresse des Computers ein.
     2. Überprüfen Sie die Seiten zur Port-Weiterleitung, und deaktivieren bzw. entfernen Sie die Einträge zum Forwarding. Speichern Sie diese Informationen, falls Sie sie zu einem späteren Zeitpunkt verwenden möchten.
   - Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

9. ***Ich habe das Passwort vergessen bzw. die Aufforderung zur Eingabe des Passworts wird jedes Mal angezeigt, wenn ich die Einstellungen für das Gateway speichere.***
   - Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste 10 Sekunden lang gedrückt halten. Wenn Sie immer noch bei jedem Speichern der Einstellungen zur Eingabe des Passworts aufgefordert werden, führen Sie die folgenden Schritte aus:
     1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Geben Sie den Standardbenutzernamen und das Standardpasswort **admin** ein, und rufen Sie unter **Administration** (Verwaltung) die Registerkarte **Management** (Verwaltungsfunktionen) auf.
     2. Geben Sie in das Feld für das Gateway-Passwort ein anderes Passwort ein. Geben Sie anschließend das gleiche Passwort in das zweite Feld ein, um es dadurch zu bestätigen.
     3. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern).

10. ***Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?***
    Wenn Sie Proxy-Einstellungen verwenden, müssen Sie diese auf Ihrem Computer deaktivieren. Da es sich bei dem Gateway um das Gateway für die Internetverbindung handelt, benötigt der Computer keine Proxy-Einstellungen für den Zugriff auf das Internet. Führen Sie die folgenden Anweisungen aus, um sicherzustellen, dass Sie keine Proxy-Einstellungen verwenden und der verwendete Browser direkt eine Verbindung mit dem LAN herstellt.

- Für Benutzer von Microsoft Internet Explorer 5.0 oder höher:
  1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Internetoptionen**.
  2. Klicken Sie auf die Registerkarte **Verbindungen**.
  3. Klicken Sie auf die Schaltfläche **LAN-Einstellungen**, und deaktivieren Sie alle aktivierten Optionen.
  4. Klicken Sie auf die Schaltfläche **OK**, um zum vorherigen Fenster zu wechseln.
  5. Aktivieren Sie die Option **Keine Verbindung wählen**. Dadurch werden alle Popup-Fenster für DFÜ-Verbindungen für PPPoE-Benutzer entfernt.

- Für Benutzer von Netscape 6 oder höher:
  1. Starten Sie **Netscape Navigator**, und klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**.
  2. Stellen Sie sicher, dass in diesem Fenster die Option **Direkte Verbindung zum Internet** ausgewählt ist.
  3. Schließen Sie alle Fenster, um den Vorgang zu beenden.

11. Ich muss das Gateway auf die Werkseinstellungen zurücksetzen, um den Vorgang noch einmal von vorn zu beginnen.

Halten Sie die Reset-Taste 10 Sekunden lang gedrückt. Dadurch werden die Interneteinstellungen, das Passwort, die Forwarding-Funktion sowie weitere Einstellungen des Gateways auf die Werkseinstellungen zurückgesetzt. Anders ausgedrückt: Das Gateway greift auf die werkseitigen Konfigurationseinstellungen zurück.

12. Ich möchte die Firmware aktualisieren.

Um die aktuellsten Funktionen für Ihre Firmware zu erhalten, gehen Sie auf die internationale Website von Linksys und laden Sie die neueste Firmware unter www.linksys.com/international herunter.

- Führen Sie die folgenden Schritte aus:
  1. Wählen Sie auf der internationalen Website von Linksys unter http://www.linksys.com/international Ihre Region bzw. Ihr Land aus.
  2. Klicken Sie auf die Registerkarte **Products** (Produkte), und wählen Sie das Gateway aus.
  3. Klicken Sie auf der Website des Gateways auf **Firmware**, und laden Sie anschließend die aktuelle Firmware für das Gateway herunter.
  4. Um die Firmware zu aktualisieren, führen Sie die in „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“ im Abschnitt **Administration** (Verwaltung) aufgeführten Schritte durch.

13. Die Aktualisierung der Firmware ist fehlgeschlagen bzw. die Netzstrom-LED blinkt.

Die Aktualisierung der Firmware kann aus mehreren Gründen fehlschlagen. Führen Sie diese Schritte aus, um die Firmware zu aktualisieren bzw. das Blinken der Netzstrom-LED zu stoppen:

- Wenn die Aktualisierung der Firmware fehlgeschlagen ist, verwenden Sie das TFTP-Programm (das Programm wurde zusammen mit der Firmware heruntergeladen). Öffnen Sie die zusammen mit der Firmware und dem TFTP-Programm heruntergeladene PDF-Datei, und befolgen Sie die darin aufgeführten Anweisungen.

- Legen Sie eine statische IP-Adresse für Ihren Computer fest. Weitere Informationen hierzu finden Sie unter „1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?“. Verwenden Sie für den Computer die folgenden Einstellungen für die IP-Adresse:
  IP-Adresse: 192.168.1.50
  Subnetzmaske: 255.255.255.0
  Gateway: 192.168.1.1
- Nehmen Sie die Aktualisierung mithilfe des TFTP-Programms oder der Registerkarte **Administration** (Verwaltung) im webbasierten Dienstprogramm des Gateways vor.

14. Das PPPoE-Protokoll des DSL-Anbieters wird stets unterbrochen.

PPPoE ist keine dedizierte oder stets aktive Verbindung. Die DSL-Verbindung kann durch den ISP getrennt werden, wenn die Verbindung einige Zeit inaktiv war, ähnlich wie bei einer normalen Telefon-DFÜ-Verbindung zum Internet.

- Es steht eine Setup-Option zur Aufrechterhaltung der Verbindung zur Verfügung. Diese Option funktioniert möglicherweise nicht immer, Sie müssen daher die Verbindung regelmäßig neu herstellen.
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)
  3. Wählen Sie im Setup-Fenster die Option **Keep Alive** (Verbindung aufrechterhalten) aus, und legen Sie für die Option **Redial Period** (Wahlwiederholung) 20 Sekunden fest.
  4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern). Klicken Sie auf die Registerkarte **Status** (Status), und klicken Sie auf Schaltfläche **Connect** (Verbinden).
  5. Möglicherweise wird **Connecting** (Verbindung wird hergestellt) als Anmeldestatus angezeigt. Drücken Sie die F5-Taste, um den Bildschirm zu aktualisieren, bis **Connected** (Verbunden) als Anmeldestatus angezeigt wird.
  6. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.
- Falls die Verbindung erneut unterbrochen wird, führen Sie die Schritte 1 bis 6 aus, um die Verbindung wiederherzustellen.

15. Ich kann weder auf meine E-Mail noch auf das Internet oder auf das VPN zugreifen, oder ich bekomme nur beschädigte Daten aus dem Internet.

Sie müssen den Wert für die MTU-Einstellung (*Maximum Transmission Unit*; Maximale Übertragungseinheit) anpassen. Die maximale Übertragungseinheit wird standardmäßig automatisch festgelegt.

- Wenn Sie Schwierigkeiten haben, führen Sie folgende Schritte aus:
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)

3. Wählen Sie für die MTU-Option **Manual** (Manuell) aus. Geben Sie in das Feld **Size** (Größe) den Wert 1492 ein.
4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.

- Wenn das Problem weiterhin besteht, ändern Sie den MTU-Wert auf einen anderen Wert. Verwenden Sie aus der folgenden Liste jeweils einen Wert in der angegebenen Reihenfolge, bis Ihr Problem gelöst ist:
  1462
  1400
  1362
  1300

16. Die Netzstrom-LED leuchtet durchgehend.

Die Netzstrom-LED leuchtet auf, wenn das Gerät erstmals eingeschaltet wird. Zwischenzeitlich fährt der Computer hoch und wird auf einen ordnungsgemäßen Betrieb hin geprüft. Nach dem Überprüfungsvorgang leuchtet die LED konstant, wodurch der ordnungsgemäße Betrieb angezeigt wird. Wenn die LED immer noch blinkt, funktioniert das Gerät nicht ordnungsgemäß. Führen Sie einen Firmware-Flash durch, indem Sie dem Computer eine statische IP-Adresse zuweisen, und aktualisieren Sie anschließend die Firmware. Verwenden Sie hierfür die folgenden Einstellungen: IP-Adresse: 192.168.1.50, Subnetzmaske: 255.255.255.0.

17. Bei Eingabe einer URL- oder IP-Adresse erhalte ich eine Meldung, dass eine Zeitüberschreitung vorliegt, bzw. die Aufforderung, den Vorgang erneut auszuführen.

- Prüfen Sie, ob Sie den Vorgang auf einem anderen Computer ausführen können. Ist dies der Fall, stellen Sie sicher, dass die IP-Einstellungen Ihres Computers korrekt sind (IP-Adresse, Subnetzmaske, Standardgateway und DNS). Starten Sie den Computer, bei dem das Problem aufgetreten ist, erneut.
- Falls der Computer korrekt konfiguriert ist, jedoch immer noch nicht funktioniert, überprüfen Sie das Gateway. Überprüfen Sie, ob es richtig angeschlossen und eingeschaltet ist. Stellen Sie die Verbindung mit dem Gateway her, und überprüfen Sie die Einstellungen. (Wenn Sie keine Verbindung herstellen können, prüfen Sie die LAN-Verbindung und die Stromversorgung.)
- Wenn das Gateway korrekt konfiguriert ist, prüfen Sie Ihre Internetverbindung (Kabel-/ADSL-Modem usw.), um den ordnungsgemäßen Betrieb des Gateways zu überprüfen. Sie können das Gateway entfernen, um dadurch die direkte Verbindung zu prüfen.
- Konfigurieren Sie die TCP/IP-Einstellung mithilfe einer von Ihrem ISP zur Verfügung gestellten DNS-Adresse manuell.
- Vergewissern Sie sich, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

18. Beim Versuch, auf das webbasierte Dienstprogramm des Gateways zuzugreifen, wird der Anmeldebildschirm nicht angezeigt. Stattdessen wird die Meldung „404 Forbidden“ (404 Nicht erlaubt) angezeigt.

Wenn Sie Internet Explorer verwenden, führen Sie die folgenden Schritte aus, bis der Anmeldebildschirm des webbasierten Dienstprogramms angezeigt wird (bei Verwendung von Netscape Navigator sind ähnliche Schritte erforderlich):

1. Klicken Sie auf **Datei**. Stellen Sie sicher, dass **Offlinebetrieb** NICHT aktiviert ist.
2. Drücken Sie die **STRG- + F5-Taste**. Dadurch wird eine Aktualisierung erzwungen und Internet Explorer veranlasst, neue und nicht gespeicherte Websites zu laden.

- Klicken Sie auf **Extras**. Klicken Sie auf **Internetoptionen**. Klicken Sie auf die Registerkarte **Sicherheit**. Klicken Sie auf die Schaltfläche **Standardstufe**. Stellen Sie sicher, dass die Sicherheitsstufe auf **Mittel** oder niedriger festgelegt ist. Klicken Sie anschließend auf die Schaltfläche **OK**.

Häufig gestellte Fragen

Wie viele IP-Adressen kann das Gateway maximal unterstützen?

Das Gateway unterstützt bis zu 253 IP-Adressen.

Unterstützt das Gateway IPSec-Passthrough?

Ja, dabei handelt es sich um eine integrierte Funktion, die standardmäßig aktiviert ist.

An welcher Stelle im Netzwerk wird das Gateway installiert?

In einer typischen Umgebung wird das Gateway zwischen der ADSL-Wandbuchse und dem LAN installiert.

Unterstützt das Gateway IPX oder AppleTalk?

Nein. TCP/IP ist der einzige Internet-Protokollstandard und ist heutzutage globaler Kommunikationsstandard. IPX ist ein Kommunikationsprotokoll von NetWare, das nur zur Weiterleitung von Nachrichten von einem Knotenpunkt zum nächsten verwendet wird. AppleTalk ist ein Kommunikationsprotokoll, das in Apple- und Macintosh-Netzwerken für LAN-zu-LAN-Verbindungen verwendet wird. Beide Protokolle können jedoch nicht zur Verbindung des Internets mit einem LAN verwendet werden.

Unterstützt die LAN-Verbindung des Gateways 100-Mbit/s-Ethernet?

Das Gateway unterstützt über den EtherFast 10/100-Switch mit Auto-Sensing-Funktion auf der LAN-Seite des Gateways auch 100 Mbit/s.

Was ist die Netzwerk-Adressen-Übersetzung, und wofür wird sie verwendet?

Die NAT-Funktion (*Network Address Translation*; Netzwerk-Adressen-Übersetzung) übersetzt mehrere IP-Adressen in einem privaten LAN in eine öffentliche Adresse, die im Internet verwendet wird. Dadurch wird die Sicherheitsstufe erhöht, da die Adresse eines mit dem privaten LAN verbundenen Computers nie an das Internet übertragen wird. Darüber hinaus ermöglicht der Einsatz von NAT die Verwendung kostengünstiger Internetverbindungen, wenn nur eine TCP/IP-Adresse vom ISP zur Verfügung gestellt wurde. So können Benutzer mehrere private Adressen hinter einer einzigen vom ISP zur Verfügung gestellten Adresse verwenden.

Unterstützt das Gateway auch andere Betriebssysteme als Windows 98 SE, ME, 2000 oder XP?

Ja. Linksys bietet jedoch derzeit keinen technischen Kundendienst hinsichtlich Installation, Konfiguration oder Fehlersuche für andere Betriebssysteme als die Windows-Betriebssysteme an.

Unterstützt das Gateway die ICQ-Dateiübertragung?

Ja, führen Sie folgende Schritte dazu aus: Klicken Sie auf das Menü **ICQ**, **Preference** (Einstellungen) und auf die Registerkarte **Connections** (Verbindungen). Aktivieren Sie dann die Option **I am behind a firewall or proxy** (Ich bin hinter einer Firewall oder einem Proxy). Legen Sie nun in den Einstellungen für die Firewall für die Zeitüberschreitung 80 Sekunden fest. Der Internetbenutzer kann nun Dateien an Benutzer hinter dem Gateway senden.

Ich habe einen Unreal Tournament-Server eingerichtet, andere Benutzer im LAN können sich jedoch nicht mit dem Server verbinden. Was muss ich tun?

Nach der Installation eines dedizierten Unreal Tournament-Servers müssen Sie eine statische IP-Adresse für jeden Computer im LAN erstellen sowie die Ports 7777, 7778, 7779, 7780, 7781 und 27900 an die IP-Adresse des Servers weiterleiten. Sie können hierfür auch einen Bereich zwischen 7777 und 27900 festlegen. Um die Funktion für UT Server Admin zu verwenden, müssen Sie einen weiteren Port weiterleiten. (Das kann Port 8080 sein, der jedoch für die Remote-Verwaltung verwendet wird. Sie müssen diese Funktion u. U. deaktivieren.) Legen Sie anschließend in der Datei SERVER.INI im Abschnitt [UWeb.WebServer] für „ListenPort“ den Wert 8080 (in Übereinstimmung mit dem oben erwähnten zugeordneten Port) und für „ServerName“ die von Ihrem ISP zur Verfügung gestellte IP-Adresse des Gateways fest.

Können mehrere Spieler im LAN auf einen Spieleserver zugreifen und mit nur einer öffentlichen IP-Adresse gleichzeitig spielen?

Das hängt vom verwendeten Netzwerkspiel bzw. dem verwendeten Server ab. So unterstützt z. B. Unreal Tournament das mehrfache Anmelden mit nur einer öffentlichen IP-Adresse.

Wie kann ich Half-Life - Team Fortress mit dem Gateway verwenden?

Der standardmäßige Client-Port für Half-Life ist 27005. Für die Computer in Ihrem LAN muss in der Befehlszeile für Half-Life-Verknüpfungen „+clientport 2700x“ hinzugefügt werden, wobei „x“ dann 6, 7, 8 usw. entspricht. Dadurch können mehrere Computer mit dem gleichen Server eine Verbindung herstellen. Problem: Bei Version 1.0.1.6 können mehrere Computer, die den gleichen CD-Schlüssel verwenden, nicht gleichzeitig mit dem Server verbunden sein, auch wenn sie sich im gleichen LAN befinden. Dieses Problem tritt bei Version 1.0.1.3 nicht auf. Beim Ausführen von Spielen muss sich der Half-Life-Server jedoch nicht in der DMZ befinden. Es muss lediglich der Port 27015 an die lokale IP-Adresse des Server-Computers weitergeleitet werden.

Die Website reagiert nicht, heruntergeladene Dateien sind beschädigt, oder es werden nur unleserliche Zeichen auf dem Bildschirm angezeigt. Was muss ich tun?
Legen Sie für Ihren Ethernet-Adapter 10 Mbit/s bzw. den Halbduplex-Modus fest, und deaktivieren Sie als vorübergehende Maßnahme für den Ethernet-Adapter die Funktion zur automatischen Aushandlung. (Rufen Sie über die Netzwerksystemsteuerung die Registerkarte für die erweiterten Eigenschaften des Ethernet-Adapters auf.) Stellen Sie sicher, dass die Proxy-Einstellung im Browser deaktiviert ist. Weitere Informationen erhalten Sie unter www.linksys.com/international.

Was kann ich tun, wenn alle Maßnahmen bei einer fehlgeschlagenen Installation erfolglos bleiben?
Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste drücken, bis die Netzstrom-LED aufleuchtet und wieder erlischt. Setzen Sie das ADSL-Modem zurück, indem Sie es aus- und erneut einschalten. Laden Sie die neueste Firmware-Version über die internationale Website von Linksys unter www.linksys.com/international herunter, und nehmen Sie die Aktualisierung vor.

Wie erhalte ich Informationen zu neuen Aktualisierungen der Gateway-Firmware?
Sämtliche Aktualisierungen für Linksys-Firmware werden auf der internationalen Website von Linksys unter www.linksys.com/international veröffentlicht und können kostenlos heruntergeladen werden. Verwenden Sie zur Aktualisierung der Gateway-Firmware die Registerkarte **System** des webbasierten Dienstprogramms des Gateways. Wenn die Internetverbindung des Gateways zufriedenstellend funktioniert, besteht keine Notwendigkeit, eine neuere Firmware-Version herunterzuladen, es sei denn, Sie möchten neue Funktionen der aktualisierten Version verwenden.

Funktioniert das Gateway in einer Macintosh-Umgebung?
Ja, Sie können jedoch nur über Internet Explorer 4.0 bzw. Netscape Navigator 4.0 oder höher für Macintosh auf die Setup-Seiten des Gateways zugreifen.

Ich kann die Seite für die Webkonfiguration des Gateways nicht aufrufen. Was kann ich tun?
Sie müssen möglicherweise die Proxy-Einstellungen in Ihrem Internet-Browser, z. B. Netscape Navigator oder Internet Explorer, entfernen. Weitere Anweisungen erhalten Sie in der Dokumentation zu Ihrem Browser. Stellen Sie sicher, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

Was bedeutet DMZ-Hosting?
Mithilfe der DMZ (*Demilitarized Zone*; Entmilitarisierte Zone) kann über eine IP-Adresse (d. h. über einen Computer) eine Verbindung zum Internet hergestellt werden. Für einige Anwendungen ist es erforderlich, dass mehrere TCP/IP-Ports geöffnet sind. Es ist empfehlenswert, dass Sie zur Verwendung des DMZ-Hostings für Ihren Computer eine statische IP-Adresse festlegen. Weitere Informationen zum Ermitteln einer LAN-IP-Adresse finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

Verwenden bei DMZ-Hosting sowohl Benutzer als auch Gateway die öffentliche IP-Adresse?
Nein.

Leitet das Gateway PPTP-Datenpakete oder PPTP-Sitzungen aktiv weiter?
Durch das Gateway werden PPTP-Datenpakete weitergeleitet.

Ist das Gateway auch plattformübergreifend einsetzbar?
Jede Plattform, die Ethernet und TCP/IP unterstützt, ist mit dem Gateway kompatibel.

Wie viele Ports können gleichzeitig weitergeleitet werden?
Das Gateway kann theoretisch 520 Sitzungen gleichzeitig ausführen, Sie können jedoch nur 10 Anschlussbereiche weiterleiten.

Über welche erweiterten Funktionen verfügt das Gateway?
Zu den erweiterten Funktionen des Gateways zählen u. a. erweiterte Wireless-Einstellungen, Filter, Port-Weiterleitung, Routing und DDNS.

Wie viele VPN-Sitzungen unterstützt das Gateway maximal?
Die maximale Anzahl hängt von vielen Faktoren ab. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen; je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.

Wie kann ich überprüfen, ob ich über statische oder DHCP-IP-Adressen verfüge?
Wenden Sie sich an Ihren ISP, um diese Informationen zu erhalten.

Wie kann ich mIRC mit dem Gateway verwenden?
Legen Sie in der Registerkarte **Port Forwarding** (Port-Weiterleitung) den Wert 113 für den Computer fest, auf dem Sie mIRC verwenden möchten.

Kann das Gateway als DHCP-Server eingesetzt werden?
Ja. Das Gateway verfügt über eine integrierte DHCP-Server-Software.

Kann ich Anwendungen von standortfernen Computern über das Wireless-Netzwerk ausführen?
Dies ist abhängig davon, ob die Anwendung für die Verwendung in Netzwerken entwickelt wurde. Informationen dazu, ob die Anwendung in Netzwerken verwendet werden kann, finden Sie in der Dokumentation der entsprechenden Anwendung.

Was ist der IEEE 802.11g-Standard?
Dies ist ein IEEE-Standard für Wireless-Netzwerke. Mit dem 802.11g-Standard können Geräte von unterschiedlichen Herstellern im Wireless-Netzwerk miteinander kommunizieren, sofern die Geräte mit dem 802.11g-Standard kompatibel sind. Durch den 802.11g-Standard ist eine maximale Datenübertragungsrate von 54 Mbit/s und eine Betriebsfrequenz von 2,4 GHz vorgegeben.

Welche IEEE 802.11b- und 802.11g-Funktionen werden unterstützt?

Das Produkt unterstützt die folgenden IEEE 802.11b- und IEEE 802.11g-Funktionen:

- CSMA/CA sowie das Acknowledge-Protokoll
- Multi-Channel-Roaming
- Automatische Ratenauswahl
- RTS/CTS
- Fragmentierung
- Energieverwaltung

Es unterstützt zudem die OFDM-Technologie für 802.11g-Netzwerke.

Was bedeutet Ad-Hoc-Modus?

Wenn für ein Wireless-Netzwerk der Ad-Hoc-Modus festgelegt ist, sind die Wireless-Computer so konfiguriert, dass sie ohne Access Point direkt miteinander kommunizieren (Peer-to-Peer).

Was bedeutet Infrastrukturmodus?

Wenn für ein Wireless-Netzwerk der Infrastrukturmodus festgelegt wurde, ist es so konfiguriert, dass es über einen Wireless Access Point mit Netzwerken kommuniziert.

Was ist Roaming?

Roaming ermöglicht Benutzern von tragbaren Computern einen reibungslosen Datenaustausch beim Zurücklegen von Entfernungen, die nicht von einem einzigen Access Point abgedeckt werden können. Vor Verwendung des Roaming muss der Computer auf die gleiche Kanalnummer wie der Access Point des entsprechenden Empfangsbereichs gesetzt werden.

Um eine dauerhafte nahtlose Verbindung zu erzielen, muss das Wireless-LAN eine Reihe an unterschiedlichen Funktionen besitzen. So müssen z. B. alle Nachrichten von jedem Knoten und jedem Access Point bestätigt werden. Jeder Knoten muss den Kontakt mit dem Wireless-Netzwerk aufrechterhalten, auch wenn keine Datenübertragung stattfindet. Um diese Funktionen gleichzeitig verwenden zu können, ist eine dynamische Funkfrequenz-Netzwerktechnologie erforderlich, mit der Access Points und Knoten miteinander verknüpft werden. In solchen Systemen sucht der Endknoten des Benutzers nach dem jeweils besten Zugriff auf das System. Zunächst werden Faktoren wie Signalstärke und -qualität, die aktuelle Nachrichtenmenge, die von jedem Access Point verarbeitet wird, und die Entfernung zwischen jedem Access Point zum verdrahteten Backbone ausgewertet. Anschließend ermittelt der Knoten auf Grundlage dieser Informationen den geeigneten Access Point und registriert dessen Adresse. Die Kommunikation zwischen Knoten und Host-Computer kann in beide Richtungen des Backbones verlaufen.

Bei fortschreitender Kommunikation prüft der Funkfrequenz-Sender des Endknotens in regelmäßigen Abständen, ob eine Verbindung mit dem ursprünglichen Access Point vorliegt oder ob ein neuer Access Point gesucht werden soll. Wenn ein Knoten keine Bestätigung des ursprünglichen Access Point mehr erhält, wird eine neue Verbindungssuche gestartet. Wenn ein neuer Access Point gefunden wurde, wird dessen Adresse registriert und die Kommunikation fortgesetzt.

Was bedeutet ISM-Band?

Die FCC-Behörde und die jeweiligen Behörden außerhalb der USA haben Bestimmungen hinsichtlich der Bandbreite für eine nicht durch Lizenzen abgedeckte Verwendung im ISM-Band erlassen. Die Frequenz liegt bei ca. 2,4 GHz und kann weltweit genutzt werden. Mit dieser wahrlich revolutionären Maßnahme können nun problemlos High Speed-Wireless-Funktionen von Benutzern weltweit genutzt werden.

Was bedeutet Bandspreizung?

Die Technologie der Bandspreizung (*Spread Spectrum Technology*) ist eine vom Militär entwickelte Breitband-Funkfrequenz-Technologie, die für zuverlässige, sichere und störresistente Kommunikationssysteme eingesetzt werden kann. Bei dieser Technologie werden gewisse Abstriche bei der Bandbreiteneffizienz hingenommen, um eine höhere Zuverlässigkeit, Integrität und Sicherheit zu erreichen. Es wird hier also eine größere Bandbreite als bei der Schmalbandübertragung verwendet. Im Gegenzug wird jedoch ein Signal erreicht, das lauter und einfacher zu lokalisieren ist, allerdings unter der Voraussetzung, dass der Empfänger die Parameter des mittels Bandspreizung übertragenen Signals kennt. Wenn ein Empfänger nicht auf die richtige Frequenz eingestellt ist, scheint ein mittels Bandspreizung übertragenes Signal nichts anderes als ein Hintergrundgeräusch zu sein. Es stehen zwei unterschiedliche Verfahren für die Bandspreizung zur Verfügung: DSSS (*Direct Sequence Spread Spectrum*; Direkte Bandspreizung) und FHSS (*Frequency Hopping Spread Spectrum*; Frequenzsprungverfahren).

Was ist DSSS? Was ist FHSS? Worin liegt der Unterschied?

Bei FHSS wird ein Schmalbandträger verwendet, der nach einem für Sender und Empfänger bekannten Muster die Frequenz ändert. Bei ordnungsgemäßer Synchronisation wird jeweils ein einziger logischer Kanal aufrechterhalten. Unerwünschten Empfängern erscheint das FHSS-Signal als kurzzeitiges Impulsrauschen. DSSS generiert ein redundantes Bitmuster für jedes zu übertragende Bit. Dieses Bitmuster wird „Chip“ oder „Chipping Code“ genannt. Je länger der Chip ist, desto größer ist die Wahrscheinlichkeit, dass die ursprüngliche Information wieder generiert werden kann. Auch wenn ein oder mehrere Bits im Chip während der Übertragung beschädigt wurden, können diese durch eine statistische Technik im Empfänger regeneriert werden und müssen daher nicht nochmals übertragen werden. Unerwünschten Empfängern erscheint das DSSS-Signal als schwaches Breitbandrauschen und wird von den meisten Schmalbandempfängern ignoriert.

Können die Daten bei der Funkübertragung abgefangen werden?

WLAN verfügt über zweifachen Schutz im Sicherheitsbereich. Im Hardwarebereich sorgt DSSS-Technologie (*Direct Sequence Spread Spectrum*; Direkte Bandspreizung) für die integrierte Sicherheitsfunktion der Verschlüsselung. Im Softwarebereich bietet WLAN die WEP-Verschlüsselungsfunktion, um die Sicherheit zu erhöhen und die Zugriffssteuerung zu verbessern.

Was ist WEP?

WEP ist die Abkürzung für *Wired Equivalent Privacy*. Hierbei handelt es sich um einen Datenschutzmechanismus, der auf einem 64-Bit- oder 128-Bit-Algorithmus mit gemeinsam verwendetem Schlüssel basiert und im IEEE 802.11-Standard festgelegt ist.

Was ist eine MAC-Adresse?
Eine MAC-Adresse (*Media Access Control*) ist eine eindeutige Nummer, die jedem Ethernet-Netzwerkgerät, wie z. B. einem Netzwerkadapter, vom Hersteller zugewiesen wird und mit der das Gerät im Netzwerk auf Hardware-Ebene identifiziert werden kann. Aus praktischen Gründen wird diese Nummer dauerhaft vergeben. Im Gegensatz zu IP-Adressen, die sich bei jeder Anmeldung des Computers beim Netzwerk ändern können, bleibt die MAC-Adresse eines Geräts stets gleich und ist dadurch eine äußerst nützliche Kennung im Netzwerk.

Wie setze ich das Gateway zurück?
Halten Sie die Reset-Taste auf der Rückseite des Gateways ca. 10 Sekunden lang gedrückt. Dadurch wird das Gateway auf die Werkseinstellungen zurückgesetzt.

Wie behebe ich einen Signalverlust?
Sie können die genaue Reichweite Ihres Wireless-Netzwerks nur durch Testen bestimmen. Jedes Hindernis zwischen dem Gateway und einem Wireless-Computer führt zu Signalverlust. Durch verbleites Glas, Metall, Betonböden, Wasser und Wände werden Signale behindert und die Reichweite vermindert. Verwenden Sie das Gateway und den Wireless-Computer zunächst im gleichen Zimmer, und vergrößern Sie dann schrittweise den Abstand zwischen beiden Geräten, um so die maximale Reichweite in Ihrer Umgebung zu bestimmen.

Verwenden Sie auch unterschiedliche Kanäle, da so Störungen ausgeschlossen werden, die nur einen Kanal betreffen.

Die Signalstärke ist absolut ausreichend, das Netzwerk wird jedoch nicht angezeigt.
Die Funktion **WEP** ist vermutlich im Gateway, jedoch nicht im Wireless-Adapter (oder umgekehrt) aktiviert. Stellen Sie sicher, dass die gleichen WEP-Schlüssel und -Ebenen (64 bzw. 128) in allen Knoten in Ihrem Wireless-Netzwerk verwendet werden.

Wie viele Kanäle/Frequenzen stehen für das Gateway zur Verfügung?
In Nordamerika sind insgesamt 11 Kanäle, von 1 bis 11, verfügbar. Für andere Regionen stehen unter Umständen weitere Kanäle zur Verfügung. Dafür sind die Vorschriften der jeweiligen Region und/oder des jeweiligen Landes maßgebend.

Wenn Ihre Fragen hier nicht beantwortet wurden, finden Sie weitere Informationen auf der internationalen Linksys-Website unter
www.linksys.com/international.

Anhang B: Sicherheit im Wireless-Netzwerkbetrieb

Linksys hat es sich zum Ziel gesetzt, den Wireless-Netzwerkbetrieb für Sie so sicher und einfach wie möglich zu gestalten. Die aktuellen Produkte von Linksys bieten verschiedene Netzwerksicherheitsfunktionen. Um diese anzuwenden, müssen Sie jedoch bestimmte Schritte ausführen. Beachten Sie daher Folgendes beim Einrichten bzw. Verwenden Ihres Wireless-Netzwerks.

Vorsichtsmaßnahmen

Bei der folgenden Liste handelt es sich um eine Auflistung aller möglichen Vorsichtsmaßnahmen. Die Schritte 1 bis 5 sollten Sie unbedingt durchführen:

1. Ändern Sie die Standard-SSID.
2. Deaktivieren Sie die SSID-Übertragung.
3. Ändern Sie das Standardpasswort für das Administratorkonto.
4. Aktivieren Sie die MAC-Adressfilterung.
5. Ändern Sie die SSID regelmäßig.
6. Verwenden Sie den höchsten verfügbaren Verschlüsselungsalgorithmus. Verwenden Sie WPA (falls verfügbar). Beachten Sie, dass die Netzwerkleistung hierdurch verringert werden kann.
7. Ändern Sie die WEP-Codierschlüssel regelmäßig.



HINWEIS: Einige dieser Sicherheitsfunktionen sind nur über das Netzwerk-Gateway, den Router oder den Access Point verfügbar. Weitere Informationen finden Sie in der Dokumentation zum Gateway, Router bzw. Access Point.

Informationen zum Umsetzen dieser Sicherheitsmaßnahmen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Home-Gateways“.

Sicherheitsrisiken bei Wireless-Netzwerken

Wireless-Netzwerke sind einfach zu finden. Hacker wissen, dass Geräte für den Wireless-Netzwerkbetrieb nach so genannten Beacon-Meldungen suchen, bevor sie sich in ein Wireless-Netzwerk einklinken. Diese Meldungen, die umfassende Netzwerkinformationen wie beispielsweise die SSID (*Service Set Identifier*) des Netzwerks enthalten, lassen sich leicht entschlüsseln. Dagegen können Sie sich folgendermaßen schützen:

Ändern Sie das Administratorpasswort regelmäßig. Bedenken Sie, dass bei jedem im Wireless-Netzwerkbetrieb verwendeten Gerät die Netzwerkeinstellungen (SSID, WEP-Schlüssel usw.) in der Firmware gespeichert sind. Die Netzwerkeinstellungen können nur vom Netzwerkadministrator geändert werden. Wenn einem Hacker das Administratorpasswort bekannt wird, kann auch er diese Einstellungen ändern. Deshalb sollten Sie es ihm so schwer wie möglich machen, an diese Informationen zu gelangen. Ändern Sie das Administratorpasswort regelmäßig.

SSID: Im Zusammenhang mit der SSID ist Folgendes zu beachten:

1. Deaktivieren Sie die Übertragung.
2. Wählen Sie eine individuelle SSID.
3. Ändern Sie sie regelmäßig.

Bei den meisten Geräten für den Wireless-Netzwerkbetrieb gibt es die Option, die SSID zu übertragen. Diese Option ist zwar recht praktisch, bedeutet jedoch, dass sich jeder in Ihr Wireless-Netzwerk einklinken kann. Jeder, auch Hacker. Daher sollten Sie die SSID nicht übertragen.

Geräte für den Wireless-Netzwerkbetrieb sind werkseitig auf eine Standard-SSID eingestellt. (Die Standard-SSID von Linksys lautet „linksys".) Hacker kennen diese Standardeinstellungen und können Ihr Netzwerk darauf überprüfen. Ändern Sie Ihre SSID, indem Sie ihr einen eindeutigen Namen zuweisen, der keinerlei Bezug zu Ihrem Unternehmen oder zu den von Ihnen verwendeten Netzwerkprodukten hat.

Ändern Sie Ihre SSID regelmäßig, damit Hacker, die sich Zugriff auf Ihr Wireless-Netzwerk verschafft haben, erneut das Passwort knacken müssen.

MAC-Adressen: Aktivieren Sie die MAC-Adressfilterung. Durch die MAC-Adressfilterung wird nur Wireless-Knoten mit bestimmten MAC-Adressen der Zugriff auf das Netzwerk ermöglicht. Dies erschwert es Hackern, mit einer zufällig gewählten MAC-Adresse auf Ihr Netzwerk zuzugreifen.

WEP Encryption (WEP-Verschlüsselung). WEP (*Wired Equivalent Privacy*) wird oft als eine Art Allheilmittel im Zusammenhang mit Sicherheitsrisiken bei Wireless-Geräten angesehen. Damit werden die Fähigkeiten von WEP jedoch überschätzt. Auch WEP kann nur soweit zur Sicherheit beitragen, dass es Hackern das Eindringen erschwert.

Es gibt mehrere Methoden, um die Wirksamkeit von WEP zu optimieren:

1. Verwenden Sie die höchste Verschlüsselungsebene.
2. Verwenden Sie die Authentifizierung mit einem freigegebenen Schlüssel.
3. Ändern Sie Ihre WEP-Schlüssel regelmäßig.



WICHTIG: Jedes Gerät im Wireless-Netzwerk MUSS dasselbe Verschlüsselungsverfahren und denselben Codierschlüssel verwenden, damit das Wireless-Netzwerk ordnungsgemäß funktioniert.

WPA: Bei **WPA** (*Wi-Fi Protected Access*) handelt es sich um den neuesten und besten verfügbaren Standard für Wi-Fi-Sicherheit. Es stehen zwei Modi zur Verfügung: **Pre-Shared Key** (Vorläufiger gemeinsamer Schlüssel) und RADIUS. Im Modus Pre-Shared Key (Vorläufiger gemeinsamer Schlüssel) stehen Ihnen zwei Verschlüsselungsverfahren zur Verfügung: **TKIP** (*Temporal Key Integrity Protocol*) und **AES** (*Advanced Encryption System*). TKIP verwendet eine leistungsfähigere Verschlüsselungsmethode sowie **MIC** (*Message Integrity Code*), um das System gegen Hacker zu schützen. AES arbeitet mit einer symmetrischen Datenverschlüsselung mit 128-Bit-Blocks. RADIUS (*Remote Authentication Dial-In User Service*) verwendet einen RADIUS-Server für die Authentifizierung sowie eine dynamische TKIP-, AES- oder WEP-Verschlüsselung.

WPA/Pre-Shared Key (WPA/Vorläufiger gemeinsamer Schlüssel): Wenn Sie nicht über einen RADIUS-Server verfügen, gehen Sie wie folgt vor: Wählen Sie den gewünschten Algorithmus (**TKIP** oder **AES**) aus, geben Sie im Feld **Pre-Shared Key** (Vorläufiger gemeinsamer Schlüssel) ein Passwort mit einer Länge von 8 bis 64 Zeichen ein und legen Sie für **Group Key Renewal** (Erneuerung Gruppenschlüssel) eine Zeit zwischen 0 und 99.999 Sekunden fest. Diese Zeitangabe teilt dem Gateway bzw. einem anderen Gerät mit, wie oft die Codierschlüssel auszutauschen sind.

WPA RADIUS: WPA wird in Verbindung mit einem RADIUS-Server verwendet. (Diese Vorgehensweise sollte nur verwendet werden, wenn ein RADIUS-Server mit einem Gateway oder einem anderen Gerät verbunden ist.) Wählen Sie zuerst den gewünschten WPA-Algorithmus aus (**TKIP** oder **AES**). Geben Sie die IP-Adresse und die Portnummer des RADIUS-Servers sowie den Schlüssel ein, der für die Verwendung durch das Gerät und den Server freigegeben ist. Legen Sie zuletzt den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Gerät mit, wie oft die Codierschlüssel auszutauschen sind.

RADIUS: WEP wird in Verbindung mit einem RADIUS-Server verwendet. (Diese Vorgehensweise sollte nur verwendet werden, wenn ein RADIUS-Server mit einem Gateway oder einem anderen Gerät verbunden ist.) Geben Sie zunächst die IP-Adresse und die Portnummer des RADIUS-Servers sowie den Schlüssel ein, der für die Verwendung durch das Gerät und den Server freigegeben ist. Wählen Sie dann einen WEP-Schlüssel und die WEP-Verschlüsselungsebene aus. Erzeugen Sie den WEP-Schlüssel über die Passphrase, oder geben Sie den WEP-Schlüssel manuell ein.

Die Verwendung von Verschlüsselungsfunktionen kann sich negativ auf die Netzwerkleistung auswirken. Wenn Sie jedoch sensible Daten über das Netzwerk senden, sollten Sie diese verschlüsseln.

Durch die Einhaltung dieser Sicherheitsempfehlungen können Sie ganz beruhigt arbeiten und die flexible und praktische Technologie von Linksys bedenkenlos einsetzen.

Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters

In diesem Abschnitt wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterungsfunktion des Gateways verwenden zu können. Sie können außerdem die IP-Adresse für den Ethernet-Adapter Ihres Computers ermitteln. Die IP-Adresse wird für die Filterungs-, Weiterleitungs- und DMZ-Funktionen des Gateways verwendet. Führen Sie die in diesem Anhang aufgelisteten Schritte aus, um die MAC- oder IP-Adresse des Adapters unter Windows 98, ME, 2000 bzw. XP zu ermitteln.

Anweisungen für Windows 98/ME

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen** den Eintrag „winipcfg“ ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

2. Wählen Sie im Fenster **IP-Konfiguration** den Ethernet-Adapter aus, den Sie über ein Ethernet-Netzwerkkabel der Kategorie 5 mit dem Gateway verbunden haben. Siehe Abbildung C-1.

3. Notieren Sie die Adapteradresse so, wie sie auf dem Bildschirm des Computers angezeigt wird (siehe Abbildung C-2). Sie bildet die MAC-Adresse Ihres Ethernet-Adapters und wird im hexadezimalen Format als Folge von Zahlen und Buchstaben dargestellt.

   Die MAC-Adresse/Adapteradresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-2 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf dem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-2 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf dem Computer angezeigte Adresse kann davon abweichen.



Hinweis: Die MAC-Adresse wird auch als Adapteradresse bezeichnet.



Abbildung C-1: Fenster „IP-Konfiguration“



Abbildung C-2: MAC-Adresse/ Adapteradresse

Anweisungen für Windows 2000/XP

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen** den Eintrag „cmd“ ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.



Hinweis: Die MAC-Adresse wird auch als physikalische Adresse bezeichnet.

2. Geben Sie in die Eingabeaufforderung **„**ipconfig /all“ ein. Drücken Sie die Eingabetaste.

3. Notieren Sie die physikalische Adresse so, wie sie am Computer anzeigt wird (Abbildung C-3). Diese Adresse stellt die MAC-Adresse des Ethernet-Adapters dar. Sie wird als Folge von Zahlen und Buchstaben dargestellt.

   Die MAC-Adresse/physikalische Adresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-3 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf dem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-3 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf dem Computer angezeigte Adresse kann davon abweichen.

Abbildung C-3: MAC-Adresse/physikalische Adresse

Anhang D: Aktualisieren der Firmware

So aktualisieren Sie die Gateway-Firmware:

1. Laden Sie die Aktualisierungsdatei für die Gateway-Firmware von der Website *www.linksys.com* herunter.
2. Extrahieren Sie die Datei auf den Computer.
3. Öffnen Sie das webbasierte Gateway-Dienstprogramm, und klicken Sie auf die Registerkarte **Administration** (Verwaltung).
4. Klicken Sie auf die Registerkarte **Firmware Upgrade** (Firmware aktualisieren).
5. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der extrahierten Datei zu suchen, und doppelklicken Sie auf diese Datei.
6. Klicken Sie auf die Schaltfläche **Upgrade** (Aktualisieren), und befolgen Sie die Anweisungen auf dem Bildschirm.



Abbildung D-1: Firmware aktualisieren

Anhang E: Glossar

802.11b: Ein Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 11 Mbit/s sowie eine Betriebsfrequenz von 2,4 GHz festlegt.

802.11g: Ein Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 Mbit/s und eine Betriebsfrequenz von 2,4 GHz sowie die Abwärtskompatibilität mit Geräten festlegt, die dem Standard 802.11b entsprechen.

Access Point: Ein Gerät, über das Computer und andere Geräte mit Wireless-Funktionalität mit einem verdrahteten Netzwerk kommunizieren können. Wird auch verwendet, um die Reichweite von Wireless-Netzwerken zu erweitern.

Adapter: Ein Gerät, mit dem Ihr Computer Netzwerkfunktionalität erhalten kann.

Ad-Hoc: Eine Gruppe von Wireless-Geräten, die nicht über einen Access Point, sondern direkt miteinander kommunizieren (Peer-to-Peer).

AES (*Advanced **E**ncryption **S**tandard*): Eine Sicherheitsmethode, bei der die symmetrische Datenverschlüsselung mit 128-Bit-Blocks verwendet wird.

Aktualisierung: Das Ersetzen vorhandener Software oder Firmware durch eine neuere Version.

Backbone: Der Teil des Netzwerks, der die meisten Systeme und Netzwerke miteinander verbindet und die meisten Daten verarbeitet.

Bandbreite: Die Übertragungskapazität eines bestimmten Geräts oder Netzwerks.

Bandspreizung: Weitband-Funkfrequenzmethode, die für eine zuverlässigere und sicherere Datenübertragung verwendet wird.

Beacon-Intervall: Im Wireless-Netzwerk übertragene Daten zur Synchronisierung des Netzwerks.

Bit: Eine binäre Einheit.

Breitband: Eine stets aktive, schnelle Internetverbindung.

Bridge: Ein Gerät, das verschiedene Netzwerke miteinander verbindet.

Browser: Eine Anwendung, mit der auf alle im World Wide Web enthaltenen Informationen interaktiv zugegriffen werden kann.

Byte: Eine Dateneinheit, die üblicherweise aus acht Bits besteht.

CSMA/CA (***C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance*): Eine Datenübertragungsmethode, die verwendet wird, um Datenkollisionen zu verhindern.

CTS (***C**lear **T**o **S**end*): Ein von einem Wireless-Gerät gesendetes Signal, das angibt, dass das Gerät für Daten empfangsbereit ist.

Daisy Chain (Verkettung): Eine Methode, bei der Geräte in Reihe (in einer Kette) miteinander verbunden werden.

Datenbank: Eine Datensammlung, die so organisiert ist, dass die enthaltenen Daten schnell und einfach verwaltet und aktualisiert werden können sowie problemlos abrufbar sind.

DDNS (***D**ynamic **D**omain **N**ame **S**ystem*): Ermöglicht das Hosten von Websiten, FTP-Servern oder E-Mail-Servern mit festen Domänennamen (z. B. www.xyz.com) und dynamischen IP-Adressen.

DHCP (***D**ynamic **H**ost **C**onfiguration **P**rotocol*): Ein Netzwerkprotokoll, mit dem Administratoren Netzwerkcomputern temporäre IP-Adressen zuweisen können, indem sie IP-Adressen für einen bestimmten Zeitraum an Benutzer „vermieten" statt ihnen eine permanente IP-Adresse zuzuweisen.

DMZ (***D**e**m**ilitarized **Z**one*): Hebt den Firewall-Schutz des Routers für einen PC auf, so dass dieser im Internet „sichtbar" wird.

DNS (***D**omain **N**ame **S**erver*): Die IP-Adresse des Servers Ihres Internetdienstanbieters, der die Namen von Websites in IP-Adressen übersetzt.

Domäne: Ein spezifischer Name für ein Netzwerk aus mehreren Computern.

DSL (***D**igital **S**ubscriber **L**ine*): Eine stets aktive Breitbandverbindung über herkömmliche Telefonleitungen.

DSSS (***D**irect-**S**equence **S**pread-**S**pectrum*): Eine Frequenzübertragungstechnologie, die ein redundantes Bit-Muster verwendet, um die Wahrscheinlichkeit von Datenverlusten bei der Übertragung zu senken.

DTIM (***D**elivery **T**raffic **I**ndication **M**essage*): Eine in Datenpaketen enthaltene Nachricht, die zur Verbesserung der Effizienz von Wireless-Verbindungen beitragen kann.

Durchsatz: Die Datenmenge, die in einem bestimmten Zeitraum erfolgreich von einem Knoten an einen anderen übertragen werden kann.

Dynamische IP-Adresse: Eine von einem DHCP-Server zugewiesene temporäre IP-Adresse.

EAP (***E**xtensible **A**uthentication **P**rotocol*): Ein allgemeines Authentifizierungsprotokoll zur Steuerung des Netzwerkzugriffs. Viele spezielle Authentifizierungsmethoden greifen auf dieses Protokoll zurück.

EAP-PEAP (***E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifzierungsmethode, bei der eine Kombination aus digitalen Zertifikaten und einem anderen System, z. B. Passwörter, verwendet wird.

EAP-TLS (***E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity*): Eine gegenseitige Authentifizierungsmethode, bei der digitale Zertifikate verwendet werden.

Ethernet: Ein Netzwerkprotokoll, mit dem festgelegt wird, wie Daten auf gängigen Übertragungsmedien gespeichert und von dort abgerufen werden.

Finger: Ein Programm, das Ihnen den Namen angibt, der einer E-Mail-Adresse zugewiesen ist.

Firewall: Eine Gruppe von Programmen, die sich auf einem Netzwerk-Gateway-Server befindet und die Ressourcen des Netzwerks vor unberechtigten Benutzern schützt.

Firmware: Der für ein Netzwerkgerät verwendete Programmiercode.

Fragmentierung: Das Aufteilen von Paketen in kleinere Einheiten bei der Übertragung über Netzwerkmedien, die die ursprüngliche Größe des Pakets nicht unterstützen.

FTP (***F**ile **T**ransfer **P**rotocol*): Ein Protokoll für die Übertragung von Dateien über ein TCP/IP-Netzwerk.

Gateway: Ein Gerät zur Verbindung von Netzwerken mit unterschiedlichen, inkompatiblen Kommunikationsprotokollen.

Halbduplex: Datenübertragung, die über eine Leitung in beide Richtungen erfolgt, jedoch entweder in die eine oder die andere Richtung, nicht gleichzeitig in beide.

Hardware: Als Hardware bezeichnet man die physischen Geräte im Computer- und Telekommunikationsbereich sowie andere Informationstechnologiegeräte.

Herunterladen: Das Empfangen einer Datei, die über ein Netzwerk übertragen wurde.

Hochfahren: Starten von Geräten, so dass diese Befehle ausführen.

HTTP (***H**yper**T**ext **T**ransport **P**rotocol*): Kommunikationsprotokoll, mit dem Verbindungen zu Servern im World Wide Web hergestellt werden.

Infrastruktur: Ein Wireless-Netzwerk, das über einen Access Point mit einem verdrahteten Netzwerk verbunden ist.

IP (***I**nternet **P**rotocol*): Ein Protokoll zum Senden von Daten über Netzwerke.

IP-Adresse: Die Adresse, anhand der ein Computer oder ein Gerät im Netzwerk identifiziert werden kann.

IPCONFIG: Ein Dienstprogramm für Windows 2000 und Windows XP, das die IP-Adresse von bestimmten Geräten im Netzwerk anzeigt.

IPSec (***I**nternet **P**rotocol **Sec**urity*): Ein VPN-Protokoll, das für den sicheren Austausch von Paketen auf der IP-Ebene verwendet wird.

ISM-Band: Bei Übertragungen im Wireless-Netzwerkbetrieb verwendete Funkbandbreite.

ISP (***I**nternet **S**ervice **P**rovider*): Internetdienstanbieter; ein Anbieter, über den auf das Internet zugegriffen werden kann.

Kabelmodem: Ein Gerät, über das ein Computer mit dem Kabelfernsehnetzwerk verbunden wird, das wiederum eine Verbindung zum Internet herstellt.

Knoten: Ein Netzwerkknotenpunkt bzw. -verbindungspunkt, üblicherweise ein Computer oder eine Arbeitsstation.

Laden: Das Übertragen einer Datei über das Netzwerk.

LAN: Die Computer und Netzwerkprodukte, aus denen sich Ihr lokales Netzwerk zusammensetzt.

LEAP (***L**ightweight **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifizierungsmethode, bei der ein Benutzername- und Passwortsystem verwendet wird.

MAC-Adresse (***M**edia **A**ccess **C**ontrol*)**:** Die eindeutige Adresse, die ein Hersteller jedem einzelnen Netzwerkbetriebsgerät zuweist.

Mbit/s (***M**ega**bit** pro **S**ekunde*): Eine Million Bit pro Sekunde. Maßeinheit für die Datenübertragung.

mIRC: Ein unter Windows verwendetes Internet Relay Chat-Programm.

Multicasting: Das gleichzeitige Senden von Daten an mehrere Ziele.

NAT (***N**etwork **A**ddress **T**ranslation*): Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.

Netzwerk: Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam verwenden, speichern und untereinander übertragen können.

NNTP (***N**etwork **N**ews **T**ransfer **P**rotocol*): Das Protokoll, mit dem eine Verbindung zu Usenet-Gruppen im Internet hergestellt wird.

OFDM (***O**rthogonal **F**requency **D**ivision **M**ultiplexing*): Eine Frequenzübertragungstechnologie, die den Datenstrom in mehrere Datenströme von geringerer Geschwindigkeit aufteilt, die dann parallel übertragen werden, um zu verhindern, dass Informationen während der Übertragung verloren gehen.

Paket: Eine Dateneinheit, die über Netzwerke gesendet wird.

Passphrase: Wird wie ein Passwort verwendet und erleichtert die WEP-Verschlüsselung, indem für Linksys Produkte automatisch WEP-Codierschlüssel erstellt werden.

PEAP (***P**rotected **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifzierungsmethode, bei der eine Kombination aus digitalen Zertifikaten und einem anderen System, z. B. Passwörter, verwendet wird.

Ping (***P**acket **IN**ternet **G**roper*): Ein Internetdienstprogramm, mit dem bestimmt werden kann, ob eine bestimmte IP-Adresse online ist.

POP3 (***P**ost **O**ffice **P**rotocol **3***): Ein im Internet verwendeter Standard-Mail-Server.

Port: Der Anschlusspunkt an einem Computer oder Netzwerkbetriebsgerät, an den Kabel oder Adapter angeschlossen werden.

Power **o**ver **E**thernet (***PoE***): Eine Technologie, mit der über Ethernet-Netzwerkkabel sowohl Daten als auch Strom übertragen werden kann.

PPPoE (***P**oint to **P**oint **P**rotocol **o**ver **E**thernet*): Eine Art der Breitbandverbindung, die neben der Datenübertragung eine Authentifizierungsmöglichkeit (Benutzername und Passwort) bietet.

PPTP (***P**oint-to-**P**oint **T**unneling **P**rotocol*): Ein VPN-Protokoll, mit dem das Point-to-Point-Protokoll (PPP) über einen Tunnel durch das IP-Netzwerk geleitet werden kann. Dieses Protokoll wird darüber hinaus in Europa als eine Art der Breitbandverbindung verwendet.

Präambel: Teil des Wireless-Signals, mit dem der Netzwerkdatenverkehr synchronisiert wird.

Puffer: Puffer sind freigegebene oder zugewiesene Speicherbereiche zur Unterstützung und Koordinierung von verschiedenen Computer- und Netzwerkaktivitäten, damit sich diese nicht gegenseitig behindern oder aufhalten.

RADIUS (***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*): Ein Protokoll zur Überwachung des Netzwerkzugriffs mithilfe eines Authentifizierungsservers.

RJ-45 (**R**egistered **J**ack**-45**): Ethernet-Anschluss für bis zu acht Drähte.

Roaming: Die Möglichkeit, mit einem Wireless-Gerät aus einem Access Point-Bereich in einen anderen zu wechseln, ohne die Verbindung zu unterbrechen.

Router: Ein Netzwerkgerät, mit dem mehrere Netzwerke miteinander verbunden werden.

RTS (*Request To Send*): Eine Methode zur Koordination von großen Datenpaketen in einem Netzwerk mithilfe der RTS-Schwelle.

Server: Ein beliebiger Computer, der innerhalb eines Netzwerks dafür sorgt, dass Benutzer auf Dateien zugreifen, kommunizieren sowie Druckvorgänge und andere Aktionen ausführen können.

SMTP (***S**imple **M**ail **T**ransfer **P**rotocol*): Das standardmäßige E-Mail-Protokoll im Internet.

SNMP (***S**imple **N**etwork **M**anagement **P**rotocol*): Ein weit verbreitetes und häufig verwendetes Protokoll zur Netzwerküberwachung und -steuerung.

Software: Befehle für den Computer. Eine Folge von Befehlen, mit denen eine bestimmte Aufgabe ausgeführt wird, wird als „Programm“ bezeichnet.

SOHO (***S**mall **O**ffice/**H**ome **O**ffice*): Marktsegment der Geschäftkunden, die zu Hause oder in kleineren Büros arbeiten.

SPI-Firewall (***S**tateful **P**acket **I**nspection*): Eine Technologie, mit der eingehende Datenpakete vor der Weiterleitung an das Netzwerk überprüft werden.

SSID (***S**ervice **S**et **ID**entifier*): Der Name Ihres Wireless-Netzwerks.

Standard-Gateway: Ein Gerät, über das der Internetdatenverkehr Ihres LANs weitergeleitet wird.

Statische IP-Adresse: Eine feste Adresse, die einem in ein Netzwerk eingebundenen Computer oder Gerät zugewiesen ist.

Statisches Routing: Das Weiterleiten von Daten in einem Netzwerk über einen festen Pfad.

Subnetzmaske: Ein Adressencode, der die Größe des Netzwerks festlegt.

Switch: 1. Ein Daten-Switch, der Rechner mit Host-Computern verbindet, wodurch eine begrenzte Anzahl von Ports von mehreren Geräten gemeinsam genutzt werden kann. 2. Ein Gerät zum Herstellen, Trennen und Ändern der Verbindungen innerhalb von elektrischen Schaltkreisen.

TCP (***T****ransmission* ***C****ontrol* ***P****rotocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem eine Bestätigung des Empfängers der gesendeten Daten erforderlich ist.

TCP/IP (***T****ransmission* ***C****ontrol* ***P****rotocol/****I****nternet* ***P****rotocol*): Ein Satz von Anweisungen, den alle PCs für die Kommunikation über Netzwerke verwenden.

Telnet: Benutzerbefehl und TCP/IP-Protokoll zum Zugriff auf entfernte PCs.

TFTP (***T****rivial* ***F****ile* ***T****ransfer* ***P****rotocol*): Eine Version des TCP/IP-FTP-Protokolls, das über keinerlei Verzeichnis- oder Passwortfunktionalitäten verfügt.

TKIP (***T****emporal* ***K****ey* ***I****ntegrity* ***P****rotocol*): Eine Wireless-Verschlüsselungsmethode, bei der für jedes übertragene Datenpaket dynamische Codierschlüssel zur Verfügung stehen.

Topologie: Die physische Anordnung eines Netzwerks.

TX-Rate: Übertragungsrate.

UDP (***U****ser* ***D****atagram* ***P****rotocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem keine Bestätigung vom Empfänger der gesendeten Daten erforderlich ist.

URL (***U****niform* ***R****esource* ***L****ocator*): Die Adresse einer im Internet befindlichen Datei.

Verschlüsselung: Die Codierung von Daten, die über Netzwerke übertragen werden.

Vollduplex: Die Fähigkeit von Netzwerkgeräten, Daten gleichzeitig empfangen und übertragen zu können.

VPN (***V****irtual* ***P****rivate* ***N****etwork*): Eine Sicherheitsmaßnahme, mit der Daten geschützt werden, wenn sie über das Internet von einem Netzwerk in ein anderes übertragen werden.

WAN (***W****ide* ***A****rea* ***N****etwork*): Das Internet.

WEP (***W****ired* ***E****quivalent* ***P****rivacy*): Eine hochgradig sichere Methode zum Verschlüsseln von Netzwerkdaten, die in Wireless-Netzwerken übertragen werden.

WINIPCFG: Ein Dienstprogramm für Windows 98 und Windows ME, das die IP-Adresse bestimmter Netzwerkbetriebsgeräte anzeigt.

WLAN (*Wireless Local Area Network*): Eine Reihe von Computern und Geräten, die über Funkverbindungen miteinander kommunizieren.

WPA (*Wi-Fi Protected Access*): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (*Temporal Key Integrity Protocol*) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann

Anhang F: Zulassungsinformationen

FCC-Bestimmungen

Dieses Gerät wurde geprüft und entspricht den Bestimmungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Die Grenzwerte wurden so festgelegt, dass ein angemessener Schutz gegen Störungen in einer Wohngegend gewährleistet ist. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und kann diese abstrahlen. Wird es nicht gemäß den Angaben des Herstellers installiert und betrieben, kann es sich störend auf den Rundfunk- und Fernsehempfang auswirken. Es besteht jedoch keine Gewähr, dass bei einer bestimmten Installation keine Störungen auftreten. Sollte dieses Gerät Störungen des Radio- und Fernsehempfangs verursachen (was durch Ein- und Ausschalten des Geräts feststellbar ist), wird der Benutzer aufgefordert, die Störungen durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus, oder stellen Sie sie an einem anderen Ort auf.
- Erhöhen Sie den Abstand zwischen der Ausrüstung oder den Geräten.
- Schließen Sie das Gerät an eine anderen Anschluss als den des Empfängers an.
- Wenden Sie sich bei Fragen an Ihren Händler oder an einen erfahrenen Funk-/Fernsehtechniker.

FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung

Dieses Gerät erfüllt die FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung in einer nicht gesteuerten Umgebung. Dieses Gerät sollte so installiert und betrieben werden, dass der Abstand zwischen dem Radiator und Personen mindestens 20 cm beträgt.

Kanadische Industriebestimmungen

Dieses Gerät erfüllt die kanadischen Bestimmungen der Richtlinien ICES-003 und RSS210.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry Canada.

Informationen zur Einhaltung gesetzlicher Vorschriften bei 2,4-GHz-Wireless-Produkten für den Bereich der EU und anderer Länder gemäß der EU-Richtlinie 1999/5/EG (R&TTE-Richtlinie)

Konformitätserklärung zur EU-Richtlinie 1995/5/EG (R&TTE-Richtlinie)

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.

Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

Hinweise: Die vollständige Konformitätserklärung finden Sie entweder auf der CD oder in einem separaten Dokument, das diesem Produkt beigefügt ist.

Wenn Sie weitere technische Dokumente benötigen, finden Sie diesbezügliche Informationen unter „Technische Dokumente unter www.linksys.com/international“ weiter hinten in diesem Anhang.

Bei der Bewertung des Produkts hinsichtlich der Anforderung der Richtlinie 1999/5/EG kamen die folgenden Standards zur Anwendung:

- Funkausrüstung: EN 300 328
- EMV: EN 301 489-1, EN 301 489-17
- Sicherheit: EN 60950

CE-Kennzeichnung

Die Wireless-B- und Wireless-G-Produkte von Linksys sind mit der folgenden CE-Kennzeichnung, der Nummer der Überwachungs- und Zertifizierungsstelle (sofern zutreffend) und der Kennung der Klasse 2 versehen.

CE 0560 ⓘ oder CE 0678 ⓘ oder CE ⓘ

Überprüfen Sie das CE-Etikett auf dem Produkt, um die Überwachungs- und Zertifizierungsstelle zu ermitteln, die in die Bewertung einbezogen wurde.

Nationale Beschränkungen

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU-Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten, die der EU-Richtlinie 1999/5/EG folgen), mit Ausnahme der folgenden Staaten:

Belgien

Wireless-Verbindungen im Freien mit einer Reichweite über 300 m müssen beim Belgischen Institut für Postdienste und Telekommunikation (BIPT) angemeldet werden. Weitere Informationen finden Sie unter http://www.bipt.be.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT).
Visitez http://www.ibpt.be pour de plus amples détails.

Frankreich

Bei Verwendung des Produkts im Freien gelten für die Ausgangsleistung in bestimmten Bandbereichen Beschränkungen. Weitere Informationen finden Sie in Tabelle 1 oder unter http://www.art-telecom.fr/.

Dans la cas d'une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous à la table 1 ou visitez http://www.art-telecom.fr/ pour de plus amples détails.

Tabelle 1: In Frankreich zulässige Leistungspegel

Standort	**Frequenzbereich (MHz)**	**Leistung (EIRP; *Effective Isotropic Radiated Power*)**
In Gebäuden (keine Beschränkungen)	2400-2483,5	100 mW (20 dBm)
Im Freien	2400-2454 2454-2483,5	100 mW (20 dBm) 10 mW (10 dBm)

Italien

Dieses Produkt entspricht den nationalen Vorschriften für Funkschnittstellen und den in der nationalen Frequenzzuweisungstabelle für Italien aufgeführten Anforderungen. Für den Betrieb dieses 2,4-GHz-Wireless-LAN-Produkts außerhalb der Grundstücksgrenzen des Eigentümers ist eine allgemeine Genehmigung erforderlich. Weitere Informationen finden Sie unter http://www.comunicazioni.it/it/.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Beschränkungen hinsichtlich der Verwendung des Produkts

Dieses Produkt wurde ausschließlich für die Verwendung in Gebäuden entwickelt. Die Verwendung im Freien wird nicht empfohlen.

Dieses Produkt wurde für die Verwendung mit der im Lieferumfang enthaltenen standardmäßigen, integrierten bzw. externen (speziell für diesen Zweck vorgesehenen) Antenne entwickelt. Manche Anwendungen setzen jedoch unter Umständen voraus, dass Sie die Antenne(n) vom Produkt trennen und mithilfe eines Verlängerungskabels an einem anderen Ort als das Gerät installieren. Für diese Anwendungen bietet Linksys ein R-SMA-Verlängerungskabel (AC9SMA) und ein R-TNC-Verlängerungskabel (AC9TNC). Beide Kabel sind neun Meter lang. Der Verlust durch das Kabel (die Abschwächung) liegt bei 5 dB. Zur Kompensation der Abschwächung bietet Linksys außerdem die Hochleistungsantennen HGA7S (mit R-SMA-Stecker) und HGA7T (mit R-TNC-Stecker). Diese Antennen verfügen über einen Antennengewinn von 7 dBi und dürfen nur mit dem R-SMA- oder R-TNC-Verlängerungskabel eingesetzt werden.

Kombinationen von Verlängerungskabeln und Antennen, die zu einem ausgestrahlten Leistungspegel von mehr als 100 mW EIRP (*Effective Isotropic Radiated Power*) führen, sind unzulässig.

Ausgangsleistung des Geräts

Zur Einhaltung der jeweiligen nationalen Vorschriften müssen Sie u. U. die Ausgangsleistung Ihres Wireless-Geräts anpassen. Fahren Sie mit dem entsprechenden Abschnitt für Ihr Gerät fort.

Hinweise: Die Einstellungen für die Ausgangsleistung sind u. U. nicht für alle Wireless-Produkte verfügbar. Weitere Informationen finden Sie in der Dokumentation auf der Produkt-CD oder unter http://www.linksys.com/international.

Wireless-Adapter

Bei Wireless-Adaptern ist die Ausgangsleistung standardmäßig auf 100 % eingestellt. Die Ausgangsleistung der einzelnen Adapter beträgt maximal 20 dBm (100 mW), liegt aber gewöhnlich bei 18 dBm (64 mW) oder darunter. Wenn Sie die Ausgangsleistung Ihres Wireless-Adapters anpassen müssen, befolgen Sie die entsprechenden Anweisungen für das Windows-Betriebssystem Ihres Computers:

Windows XP

1. Doppelklicken Sie auf dem Desktop in der Taskleiste auf das Symbol **Drahtlose Verbindung**.
2. Öffnen Sie das Fenster *Drahtlose Netzwerkverbindung*.
3. Klicken Sie auf die Schaltfläche **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Allgemein** und dann auf die Schaltfläche **Konfigurieren**.
5. Klicken Sie im Fenster *Eigenschaften* auf die Registerkarte **Erweitert**.
6. Wählen Sie **Ausgangsleistung** aus.
7. Wählen Sie aus dem rechts angezeigten Pulldown-Menü den Prozentsatz für die Ausgangsleistung des Wireless-Adapters aus.

Windows 2000

1. Öffnen Sie das Fenster **Systemsteuerung**.
2. Doppelklicken Sie auf **Netzwerk- und DFÜ-Verbindungen**.
3. Wählen Sie Ihre aktuelle Wireless-Verbindung aus, und wählen Sie dann **Eigenschaften**.
4. Klicken Sie im Fenster *Eigenschaften* auf die Schaltfläche **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Erweitert**, und wählen Sie **Ausgangsleistung** aus.
6. Wählen Sie aus dem rechts angezeigten Pulldown-Menü die Leistungseinstellung für den Wireless-Adapter aus.

Wenn auf Ihrem Computer Windows ME oder Windows 98 ausgeführt wird, finden Sie in der Windows-Hilfe Anweisungen zum Aufrufen der erweiterten Einstellungen von Netzwerkadaptern.

Wireless Access Points, Router und andere Wireless-Produkte

Wenn Sie über einen Wireless Access Point, einen Router oder ein anderes Wireless-Produkt verfügen, verwenden Sie das zugehörige webbasierte Dienstprogramm, um die Einstellungen für die Ausgangsleistung zu konfigurieren (weitere Informationen finden Sie in der Dokumentation zum jeweiligen Produkt).

Technische Dokumente unter www.linksys.com/international

Führen Sie die folgenden Schritte aus, um auf die gewünschten technischen Dokumente zuzugreifen:

1. Navigieren Sie mit dem Browser zur Website http://www.linksys.com/international.
2. Klicken Sie auf Ihre Region.
3. Klicken Sie auf den Namen Ihres Landes.
4. Klicken Sie auf **Produkt**.
5. Klicken Sie auf die entsprechende Produktkategorie.
6. Wählen Sie ein Produkt aus.
7. Klicken Sie auf den gewünschten Dokumentationstyp. Das Dokument wird automatisch im PDF-Format geöffnet.

Hinweise: Wenn Sie Fragen zur Einhaltung gesetzlicher Vorschriften in Bezug auf diese Produkte haben oder die gewünschten Informationen nicht finden können, wenden Sie sich an die Vertriebsniederlassung vor Ort, oder rufen Sie weitere Einzelheiten unter http://www.linksys.com/international ab.

Anhang G: Garantieinformationen

Linksys sichert Ihnen für einen Zeitraum von drei Jahren (die „Gewährleistungsfrist") zu, dass dieses Linksys Produkt bei normaler Verwendung keine Material- oder Verarbeitungsfehler aufweist. Im Rahmen dieser Gewährleistung beschränken sich Ihre Rechtsmittel und der Haftungsumfang von Linksys wie folgt: Linksys kann nach eigenem Ermessen das Produkt reparieren oder austauschen oder Ihnen den Kaufpreis abzüglich etwaiger Nachlässe zurückerstatten. Diese eingeschränkte Gewährleistung gilt nur für den ursprünglichen Käufer.

Sollte sich das Produkt während der Gewährleistungsfrist als fehlerhaft erweisen, wenden Sie sich an den technischen Kundendienst von Linksys, um eine so genannte *Return Authorization Number* (Nummer zur berechtigten Rücksendung) zu erhalten. WENN SIE SICH AN DEN TECHNISCHEN KUNDENDIENST WENDEN, SOLLTEN SIE IHREN KAUFBELEG ZUR HAND HABEN. Wenn Sie gebeten werden, das Produkt einzuschicken, geben Sie die Nummer zur berechtigten Rücksendung gut sichtbar auf der Verpackung an und legen Sie eine Kopie des Originalkaufbelegs bei. RÜCKSENDEANFRAGEN KÖNNEN NICHT OHNE DEN KAUFBELEG BEARBEITET WERDEN. Der Versand fehlerhafter Produkte an Linksys erfolgt auf Ihre Verantwortung. Linksys kommt nur für Versandkosten von Linksys zu Ihrem Standort per UPS auf dem Landweg auf. Bei Kunden außerhalb der USA und Kanadas sind sämtliche Versand- und Abfertigungskosten durch die Kunden selbst zu tragen.

ALLE GEWÄHRLEISTUNGEN UND BEDINGUNGEN STILLSCHWEIGENDER ART HINSICHTLICH DER MARKTÜBLICHEN QUALITÄT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUF DIE DAUER DER GEWÄHRLEISTUNGSFRIST BESCHRÄNKT. JEGLICHE WEITEREN BEDINGUNGEN, ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN SOWOHL AUSDRÜCKLICHER ALS AUCH STILLSCHWEIGENDER ART, EINSCHLIESSLICH JEGLICHER STILLSCHWEIGENDER GEWÄHRLEISTUNG DER NICHTVERLETZUNG, WERDEN AUSGESCHLOSSEN. Einige Gerichtsbarkeiten gestatten keine Beschränkungen hinsichtlich der Gültigkeitsdauer einer stillschweigenden Gewährleistung; die oben genannte Beschränkung findet daher unter Umständen auf Sie keine Anwendung. Die vorliegende Gewährleistung sichert Ihnen bestimmte gesetzlich verankerte Rechte zu. Darüber hinaus stehen Ihnen je nach Gerichtsbarkeit unter Umständen weitere Rechte zu.

Diese Gewährleistung gilt nicht, wenn das Produkt (a) von einer anderen Partei als Linksys verändert wurde, (b) nicht gemäß den von Linksys bereitgestellten Anweisungen installiert, betrieben, repariert oder gewartet wurde oder (c) unüblichen physischen oder elektrischen Belastungen, Missbrauch, Nachlässigkeit oder Unfällen ausgesetzt wurde. Darüber hinaus kann Linksys angesichts der ständigen Weiterentwicklung neuer Methoden zum unerlaubten Zugriff und Angriff auf Netzwerke nicht gewährleisten, dass das Produkt keinerlei Schwachstellen für unerlaubte Zugriffe oder Angriffe bietet.

SOWEIT NICHT GESETZLICH UNTERSAGT, SCHLIESST LINKSYS JEGLICHE HAFTUNG FÜR VERLOREN GEGANGENE DATEN, ENTGANGENE EINNAHMEN, ENTGANGENE GEWINNE ODER SONSTIGE SCHÄDEN BESONDERER, INDIREKTER, MITTELBARER, ZUFÄLLIGER ODER BESTRAFENDER ART AUS, DIE SICH AUS DER VERWENDUNG BZW. DER NICHTVERWENDBARKEIT DES PRODUKTS (AUCH DER SOFTWARE) ERGEBEN ODER MIT DIESER ZUSAMMENHÄNGEN, UNABHÄNGIG VON DER HAFTUNGSTHEORIE (EINSCHLIESSLICH NACHLÄSSIGKEIT), AUCH WENN LINKSYS ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. DIE HAFTUNG VON LINKSYS IST STETS AUF DEN FÜR DAS PRODUKT GEZAHLTEN BETRAG BESCHRÄNKT. Die oben genannten Beschränkungen kommen auch dann zur Anwendung, wenn eine in diesem Abschnitt aufgeführte Gewährleistung oder Zusicherung ihren wesentlichen Zweck verfehlt. Einige Gerichtsbarkeiten gestatten keinen Ausschluss von bzw. keine Beschränkungen auf zufällige oder Folgeschäden; die oben genannte Beschränkung oder der oben genannte Ausschluss findet daher unter Umständen auf Sie keine Anwendung.

Die vorliegende Gewährleistung ist nur in dem Land gültig bzw. kann nur in dem Land verarbeitet werden, in dem das Produkt erworben wurde.

Richten Sie alle Anfragen direkt an: Linksys, P.O. Box 18558, Irvine, CA 92623, USA.

Anhang H: Spezifikationen

Modellnummer	WAG354G
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, G.992.1 (G.dmt), G.992.2 (G.lite), G.992.3, G.992.5, T1.413i2
Ports	Netzstrom, ADSL, Ethernet (1-4)
Taste	Eine Reset-Taste
Kabeltyp	Kat. 5 UTP
LEDs	Netzstrom, Wireless, Ethernet (1-4), DSL, Internet
Anzahl Antennen	1
Art der Steckverbindung	SMA
Abnehmbar (j/n)	Ja
Antennengewinn in dBi	2 dBi
Übertragungsleistung	18 dBm
Kanäle	13 (in den meisten Teilen Europas)
UPnP-fähig/-zertifiziert	UPnP-fähig
Sicherheitsmerkmale	Passwortgeschützte Konfiguration für Web-Zugriff PAP- und CHAP-Authentifizierung DoS-Schutz (Denial of Service) URL-Filterung sowie Blockieren von Stichwörtern, Java, ActiveX, Proxy und Cookies

	ToD-Filter (Blockieren des Zugriffs nach Zeit) VPN-Passthrough für IPSec-, PPTP- und L2TP-Protokolle WEP (128/64 Bit) mit Passphrasen-/WEP-Schlüsselerstellung Deaktivierung der SSID-Übertragung Zugriffsbeschränkung nach MAC- und IP-Adressen
WEP-Schlüssel	64 Bit, 128 Bit
Abmessungen	140 mm x 140 mm x 27 mm
Gerätegewicht	0,3 kg
Stromversorgung	12 V WS, 1 A
Zertifizierungen	CE
Betriebstemperatur	0 ºC bis 40 ºC
Lagertemperatur	-20 ºC bis 70 ºC
Betriebsfeuchtigkeit	10 % bis 85 %, nicht kondensierend
Lagerfeuchtigkeit	5 % bis 90 %, nicht kondensierend

Anhang I: Kontaktinformationen

Möchten Sie sich persönlich an Linksys wenden?
Informationen zu den aktuellen Produkten und Aktualisierungen für bereits installierte Produkte finden Sie online unter: http://www.linksys.com/international

Wenn Sie im Zusammenhang mit Linksys Produkten auf Probleme stoßen, können Sie uns unter folgenden Adressen eine E-Mail senden:

In Europa	E-Mail-Adresse
Belgien	support.be@linksys.com
Dänemark	support.dk@linksys.com
Deutschland	support.de@linksys.com
Frankreich	support.fr@linksys.com
Großbritannien & Irland	support.uk@linksys.com
Italien	support.it@linksys.com
Niederlande	support.nl@linksys.com
Norwegen	support.no@linksys.com
Österreich	support.at@linksys.com
Portugal	support.pt@linksys.com
Schweden	support.se@linksys.com
Schweiz	support.ch@linksys.com
Spanien	support.es@linksys.com

Außerhalb von Europa	E-Mail-Adresse
Lateinamerika	support.la@linksys.com
USA und Kanada	support@linksys.com



A Division of Cisco Systems, Inc.



2,4 GHz 802.11g **Sans fil G**



Modem routeur ADSL résidentiel

Guide de l'utilisateur



Modèle **WAG354G (FR)**

Copyright et marques commerciales

Comment utiliser ce Guide de l'utilisateur ?

Ce guide présentant le modem routeur ADSL résidentiel sans fil G a été conçu pour faciliter au maximum votre compréhension de la mise en réseau à l'aide du modem routeur. Les symboles suivants sont contenus dans ce Guide de l'utilisateur :



Cette coche indique un élément qui mérite une attention plus particulière lors de l'utilisation de votre modem routeur.



Ce point d'exclamation indique un avertissement et vous avertit de la possibilité d'endommagement de votre installation ou de votre modem routeur.



Ce point d'interrogation indique un rappel concernant quelque chose que vous êtes susceptible de devoir faire pour utiliser votre modem routeur.

Outre ces symboles, les définitions concernant des termes techniques sont présentées de la façon suivante :

Mot : *définition.*

Chaque figure (diagramme, capture d'écran ou toute autre image) est accompagnée d'un numéro et d'une description, comme ceci :

Figure 0-1 : Exemple de description d'une figure

Les numéros de figures et les descriptions sont également répertoriés dans la section « Liste des figures » de la « Table des matières ».

WAG354G-FR-UG-50401NC JL

Table des matières

Liste des figures

Chapitre 1 : Introduction

Accueil

Merci d'avoir choisi le modem routeur ADSL résidentiel sans fil G. Avec ce modem routeur, vous êtes en mesure d'équiper vos ordinateurs d'une connexion Internet haut débit et d'autres ressources, telles que fichiers et imprimantes. S'agissant d'un modem routeur sans fil, vous pouvez partager cet accès Internet sur le réseau câblé ou via la diffusion sans fil à 11 Mbit/s pour le routeur sans fil B ou jusqu'à 54 Mbit/s pour le modèle sans fil G.

Comment le modem routeur peut-elle vous offrir tous ces avantages ? Une fois le modem routeur connectée à Internet, ainsi qu'à vos ordinateurs et périphériques, elle est en mesure de diriger et de contrôler les communications de votre réseau.

En outre, afin de protéger vos données et votre vie privée, le modem routeur dispose d'un pare-feu avancé empêchant les intrusions par le biais d'Internet. Les transmissions sans fil peuvent être protégées par un cryptage de données puissant. Vous pouvez en outre protéger votre famille grâce aux fonctions de contrôle parental telles que les restrictions d'accès à Internet et le blocage par mot clé. Les paramètres du modem routeur peuvent aisément être configurés avec l'utilitaire Web (accessible avec votre navigateur).

Que signifie tout ceci ?

Les réseaux permettent de partager un accès Internet et des ressources informatiques. Vous pouvez connecter plusieurs ordinateurs à une même imprimante et accéder à des données stockées sur le disque dur d'un autre ordinateur. Les réseaux sont même utilisés pour les jeux vidéo multi-utilisateur. Outre leur utilité à la maison et au bureau, ils peuvent donc servir à des activités plus ludiques.

Les ordinateurs reliés à un réseau câblé constituent un réseau local ou LAN. Ils sont connectés par l'intermédiaire de câbles Ethernet, d'où le terme de réseau dit câblé. Les ordinateurs équipés de cartes ou d'adaptateurs sans fil peuvent communiquer sans la présence de câbles encombrants. En partageant les mêmes paramètres sans fil conformément à leur rayon de transmission, ils forment un réseau sans fil. On parle parfois de réseau local sans fil ou WLAN. Les fonctions sans fil du modem routeur permettent de relier vos réseaux câblé et sans fil et d'établir une communication entre eux.

Grâce à vos réseaux connectés, câblés et sans fil, et d'Internet, vous pouvez alors partager des fichiers et l'accès à Internet et même jouer. Simultanément, le modem routeur ADSL résidentiel sans fil G protège vos réseaux et empêche tout utilisateur non autorisé et indésirable d'y accéder.

Linksys vous recommande d'utiliser le CD-ROM d'installation pour la première installation du modem routeur. Si vous ne souhaitez pas exécuter l'Assistant de configuration disponible sur le CD-ROM d'installation, suivez les instructions de ce Guide pour connecter, installer et configurer le modem routeur pour relier vos différents

***wpa** (wi-fi protected access) : protocole de sécurité sans fil faisant appel au cryptage TKIP (Temporal Key Integrity Protocol) et pouvant être utilisé en association avec un serveur RADIUS.*

***Pare-feu spi** (stateful packet inspection) : technologie inspectant les paquets d'informations entrants avant de les autoriser à pénétrer le réseau.*

***pare-feu** : mesures de sécurité protégeant les ressources d'un réseau local contre toute intrusion.*

***nat** (network address translation) : la technologie NAT permet de convertir les adresses IP d'un réseau local en une adresse IP distincte sur Internet.*

***réseau** : plusieurs ordinateurs ou périphériques reliés entre eux dans le but de partager et de stocker des données et/ou de permettre la transmission de données entre plusieurs utilisateurs.*

***lan** (local area network) : les ordinateurs ou produits mis en réseau qui constituent votre réseau à domicile ou au bureau.*

réseaux. Ces instructions devraient s'avérer suffisantes et vous permettre de tirer le meilleur parti du modem routeur ADSL résidentiel sans fil G.

Contenu de ce Guide de l'utilisateur

Ce Guide de l'utilisateur présente les étapes inhérentes à l'installation et à l'utilisation du modem routeur ADSL résidentiel sans fil G.

- Chapitre 1 : Introduction
  Ce chapitre décrit les applications du modem routeur ADSL résidentiel sans fil G ainsi que le présent Guide de l'utilisateur.

- Chapitre 2 : Planification de la configuration de votre réseau
  Ce chapitre décrit les éléments de base nécessaires à la mise en place d'un réseau.

- Chapitre 3 : Présentation du modem routeur ADSL résidentiel sans fil G
  Ce chapitre décrit les caractéristiques physiques du modem routeur.

- Chapitre 4 : Connexion du modem routeur ADSL résidentiel sans fil G
  Ce chapitre vous explique pas à pas comment connecter le modem routeur à votre réseau.

- Chapitre 5 : Configuration du modem routeur ADSL résidentiel sans fil G
  Ce chapitre explique comment manipuler l'utilitaire Web pour configurer les paramètres du modem routeur.

- Annexe A : Dépannage
  Cette annexe expose quelques problèmes et leurs solutions, ainsi que les questions fréquemment posées au sujet de l'installation et de l'utilisation du modem routeur ADSL résidentiel sans fil G.

- Annexe B : Sécurité sans fil
  Cette annexe décrit les risques liés aux réseaux sans fil et propose quelques solutions en vue de réduire ces risques.

- Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet.
  Cette annexe explique comment rechercher l'adresse MAC de l'adaptateur Ethernet de votre ordinateur pour être en mesure d'utiliser la fonctionnalité de filtrage MAC et/ou la fonctionnalité de clonage des adresses MAC du modem routeur.

- Annexe D : Mise à jour du micrologiciel
  Cette annexe vous explique comment mettre à niveau le micrologiciel sur votre modem routeur si cette opération s'avère nécessaire.

- Annexe E : Glossaire
  Cette annexe propose un glossaire des termes fréquemment utilisés dans le cadre des réseaux.

- Annexe F : Réglementation
  Cette annexe fournit des informations relatives à la réglementation relative à l'utilisation du modem routeur.

- Annexe G : Informations de garantie
  Cette annexe fournit des informations relatives à la garantie du modem routeur.

- Annexe H : Spécifications
  Cette annexe décrit les spécifications techniques du modem routeur.

- Annexe I : Contacts
  Cette annexe fournit des informations sur diverses ressources Linksys que vous pouvez contacter, notamment le support technique.

Chapitre 2 : Planification de la configuration de votre réseau

Les fonctions du modem routeur

Un modem routeur est un périphérique réseau qui connecte deux réseaux entre eux.

Dans ce cas, le modem routeur connecte à Internet votre réseau local (LAN) ou un groupe d'ordinateurs situés à votre bureau ou à votre domicile. Le modem routeur traite et régule les données transmises entre ces deux réseaux.

La fonctionnalité NAT du modem routeur protège votre réseau d'ordinateurs, de manière à ce que les utilisateurs Internet publics ne puissent pas « voir » vos ordinateurs. De cette façon, votre réseau reste privé. Le modem routeur protège votre réseau en inspectant chaque paquet entrant via la port Internet avant qu'il soit transmis vers la machine appropriée du réseau. Le modem routeur inspecte les services du port Internet tels que le serveur Web, le serveur FTP ou toute autre application Internet. Si elle est autorisée à le faire, elle transmet ensuite le paquet à l'ordinateur approprié du réseau local.

N'oubliez pas que les ports du modem routeur sont connectés à deux « côtés ». Les ports LAN sont connectés à votre réseau local (LAN) et le port ADSL est connecté à Internet. Les ports LAN transmettent les données à un débit de 10/100 Mbit/s.



Figure 2-1 : Réseau

***IP** (Internet Protocol) : protocole utilisé pour transmettre des données sur un réseau*

Adresses IP

Qu'est ce qu'une adresse IP ?

IP signifie Internet Protocol. Chaque périphérique d'un réseau basé sur des adresses IP, comprenant des ordinateurs, des serveurs d'impression et des modems routeurs, requiert une adresse IP pour l'identification de son « emplacement » ou adresse sur le réseau. Elle s'applique aux connexions LAN et Internet. Il existe deux façons d'attribuer une adresse IP à vos périphériques réseau. Vous pouvez attribuer des adresses IP statiques ou utiliser le modem routeur pour attribuer dynamiquement ces adresses IP.

Adresses IP statiques

Une adresse IP statique est une adresse IP fixe que vous attribuez manuellement à un ordinateur ou à un autre périphérique du réseau. Etant donné qu'une adresse IP statique reste valide jusqu'à ce que vous la désactiviez, l'utilisation d'une adresse IP statique permet de s'assurer que le périphérique correspondant aura toujours la même



REMARQUE : Etant donné que le modem routeur est un périphérique connecté à deux réseaux, elle requiert deux adresses IP : une pour le réseau local et une pour Internet. Dans ce Guide de l'utilisateur, vous trouverez des références à l'« adresse IP Internet » et à l'« adresse IP LAN ».

Puisque le modem routeur utilise la technologie NAT, la seule adresse IP de votre réseau qui peut être « vue » à partir d'Internet est l'adresse IP Internet du modem routeur. Néanmoins, même cette adresse IP peut être bloquée afin que le modem routeur et le réseau soient invisibles sur Internet. Veuillez vous reporter à la présentation du blocage des requêtes WAN à la section Sécurité du « Chapitre 5 : Configuration du modem routeur ADSL résidentiel sans fil G ».

adresse IP tant que vous ne la changez pas. Les adresses IP statiques doivent être uniques et sont généralement utilisées avec des périphériques réseau tels que les serveurs d'ordinateurs ou les serveurs d'impression.

Etant donné que vous utilisez le modem routeur pour partager votre connexion Internet DSL, contactez votre fournisseur d'accès Internet pour savoir si une adresse IP statique à été attribuée à votre compte. Si c'est le cas, vous aurez besoin de cette adresse IP statique lors de la configuration de votre modem routeur. Vous pouvez obtenir cette information en contactant votre fournisseur d'accès Internet.

Adresses IP dynamiques

Une adresse IP dynamique est automatiquement attribuée à un périphérique du réseau, tel que des ordinateurs et des serveurs d'impression. Ces adresses IP sont dites « dynamiques » car elles sont attribuées temporairement à l'ordinateur ou au périphérique. Après un certain temps, elles expirent et peuvent être changées. Si un ordinateur se connecte au réseau (ou à Internet) et que son adresse IP dynamique a expiré, le serveur DHCP lui attribue automatiquement une nouvelle adresse IP dynamique.

Serveurs DHCP (Dynamic Host Configuration Protocol)

Les ordinateurs et tous les autres périphériques réseau utilisant des adresses IP dynamiques se voient attribuer une nouvelle adresse IP par un serveur DHCP. L'ordinateur ou le périphérique réseau qui obtient une adresse IP est appelé le client DHCP. DHCP vous évite d'avoir à attribuer des adresses IP manuellement dès qu'un nouvel utilisateur est ajouté à votre réseau.

Un serveur DHCP peut être soit un ordinateur dédié du réseau, soit un autre périphérique réseau, tel que le modem routeur. Par défaut, la fonction de serveur DHCP du modem routeur est activée.

Si vous disposez déjà d'un serveur DHCP sur votre réseau, vous devez désactiver l'un des deux serveurs DHCP. Si vous exécutez plusieurs serveurs DHCP sur votre réseau, des erreurs se produisent, telles que des conflits d'adresses IP. Pour désactiver la fonction DHCP sur le modem routeur, reportez-vous à la section relative au DHCP dans le « Chapitre 5 : Configuration du modem routeur ADSL résidentiel sans fil G ».

Chapitre 3 : Présentation du modem routeur ADSL résidentiel sans fil G

Ports et bouton Reset (Réinitialisation) du panneau latéral

Les ports et le bouton Reset (Réinitialisation) sont situés sur un panneau latéral du modem routeur.

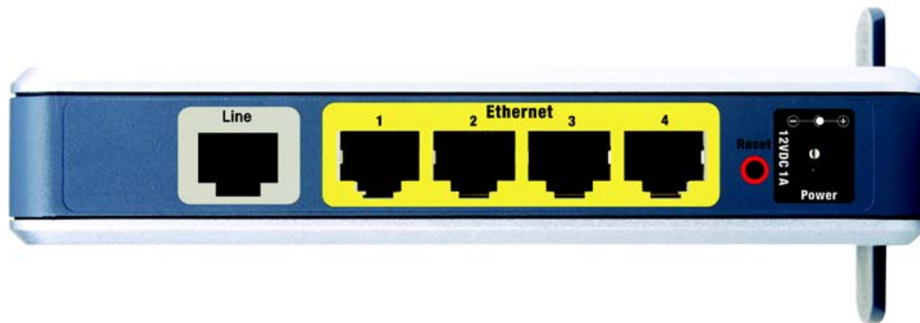


Figure 3-1 : Ports et bouton Reset (Réinitialisation) du panneau latéral

Line	Le port **Line** (LIGNE) permet de connecter la câble ADSL.
Ethernet (1-4)	Les ports **Ethernet** permettent de connecter l'appareil à vos ordinateurs et à d'autres périphériques réseau.
Bouton Reset (Réinitialisation)	Il existe deux façons de réinitialiser les paramètres d'usine de votre modem routeur : Appuyez sur le bouton **Reset** (Réinitialiser), pendant environ dix secondes ou restaurez les paramètres par défaut à partir de l'écran *Paramètres usine* de l'onglet Administration de l'utilitaire Web du modem routeur.
Power (Alimentation)	Le port **Power** (Alimentation) est l'emplacement auquel vous devez connecter l'adaptateur électrique.



IMPORTANT : La réinitialisation du modem routeur vers les paramètres d'usine supprime tous les paramètres personnalisés (connexion Internet, sans fil et autres). Ne réinitialisez pas les paramètres du modem routeur si vous souhaitez les conserver.

Voyants du panneau latéral

Les voyant du modem routeur, qui indiquent l'activité du réseau, se trouvent sur le panneau latéral.



Figure 3-2 : Voyants du panneau latéral

Power (Alimentation)	Vert. Le voyant **POWER** (Alimentation) s'allume lorsque le modem routeur est sous tension.
WIRELESS (sans fil)	Vert. Le voyant **WIRELESS** (sans fil) s'allume lorsqu'une connexion sans fil est établie. Si le voyant clignote, cela signifie que le modem routeur traite actuellement l'envoi ou la réception de données avec l'un des périphériques du réseau.
ETHERNET (1-4)	Vert. Le voyant **ETHERNET** a deux fonctions. S'il est allumé en permanence, cela signifie que le modem routeur est connectée correctement à un périphérique via le port LAN (réseau local). S'il clignote, il indique une activité réseau.
DSL	Vert. Le voyant **DSL** s'allume lorsqu'une connexion DSL est réalisée avec succès. Il clignote lorsque le modem routeur établit la connexion ADSL.
INTERNET	Vert. Le voyant **INTERNET** est vert lorsqu'une connexion au fournisseur d'accès Internet (FAI) a été établie. Le voyant **INTERNET** est rouge si la connexion au fournisseur d'accès Internet (FAI) a échoué.

Panneau supérieur

Le modem routeur est livrée avec une antenne intégrée mais vous pouvez, si vous le souhaitez, fixer une antenne facultative. (Remarque : cette antenne n'est pas encore disponible en Europe.) L'antenne Linksys 5 dBi à gain élevé pour connecteurs SMA (référence du modèle : HGA5S) est disponible pour une plage accrue. Le port SMA du modem routeur destiné à l'antenne facultative est situé sur le panneau supérieur. Pour accéder au port SMA, appuyez sur l'onglet. Pour fixer l'antenne, insérez la base de l'antenne dans le port SMA et serrez à la main, en tournant vers la droite.

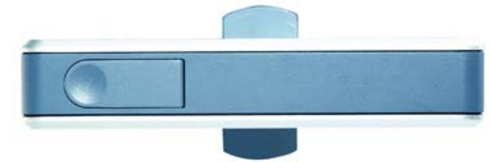


Figure 3-3 : Panneau supérieur

Antenne Linksys 5 dBi facultative (Référence du modèle : HGA5S)
Remarque : Cette antenne n'est actuellement pas disponible en Europe.

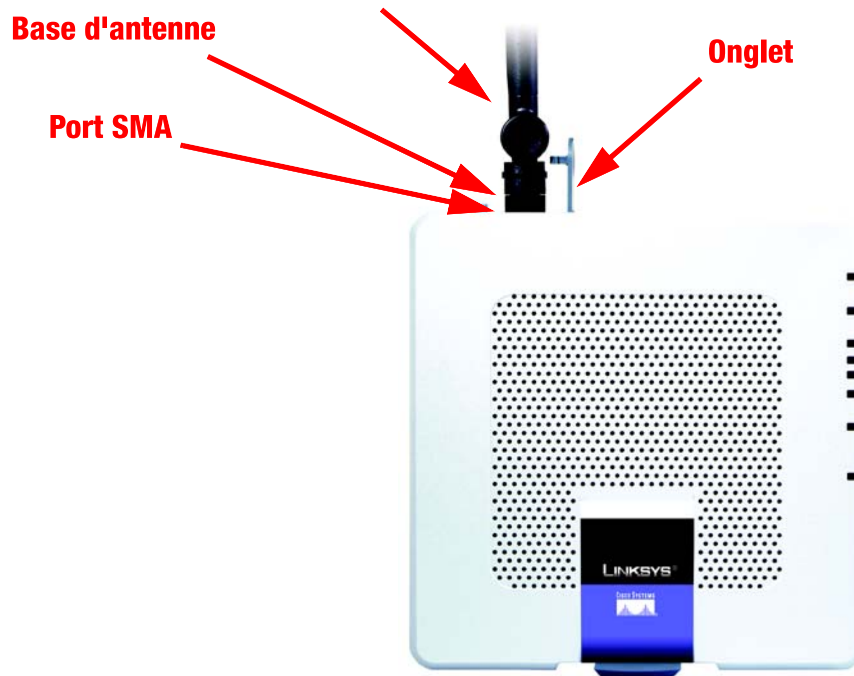


Figure 3-4 : Panneau supérieur avec antenne facultative

Panneau inférieur

Le modem routeur est munie d'un support intégré. Si vous posez le modem routeur à plat, le support peut demeurer en position fermée. Si vous préférez mettre le modem routeur en position verticale, faites pivoter le support de 90º vers la droite avant de loger le modem routeur selon vos souhaits.



Figure 3-5 : Panneau inférieur avec support en position fermée



Figure 3-6 : Modem routeur avec support

Chapitre 4 : Connexion du modem routeur ADSL résidentiel sans fil G

Présentation

Le technicien de votre fournisseur d'accès Internet doit vous avoir communiqué les données concernant le modem après avoir installé votre connexion large bande. Dans le cas contraire, contactez votre FAI.

Si vous disposez des informations de configuration correspondant à votre type de connexion Internet, vous pouvez commencer l'installation et la configuration de votre modem routeur.

Si vous souhaitez utiliser un ordinateur équipé d'un adaptateur Ethernet pour configurer le modem routeur, passez à la rubrique « Connexion câblée à un ordinateur ». Si vous souhaitez utiliser un ordinateur équipé d'un adaptateur sans fil pour configurer le modem routeur, passez à la rubrique « Connexion sans fil à un ordinateur ».

Connexion câblée à un ordinateur

1. Vérifiez que tous les appareils du réseau sont hors tension, y compris le modem routeur et tous les ordinateurs.

2. Branchez un câble téléphonique entre le port Line (Ligne) du panneau latéral du modem routeur et la prise murale de la ligne ADSL Il peut être nécessaire de placer un petit périphérique appelé microfiltre (non fourni) entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.

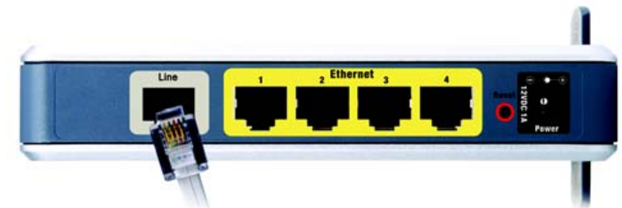


Figure 4-1 : Connexion d'une ligne ADSL



REMARQUE : Il peut être nécessaire de placer un petit périphérique appelé microfiltre (non fourni) entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.



IMPORTANT : Dans les pays où les prises téléphoniques sont utilisées avec des connecteurs RJ-11, veillez à placer les microfiltres entre le téléphone et la prise murale et **non pas** entre le modem routeur et la prise murale. Sinon, la connexion ADSL ne pourra pas être établie.

Dans les pays où les prises téléphoniques **ne sont pas** utilisées avec des connecteurs RJ-11 (par exemple, France, Suède, Suisse, Royaume-Uni, etc.), sauf pour les utilisateurs RNIS, le microfiltre doit être placé entre le modem routeur et la prise murale, car il contient le connecteur RJ-11.

Les utilisateurs de Annex B (versions E1 et DE du modem routeur) doivent utiliser le câble spécial fourni pour connecter le modem routeur à la prise murale (RJ-45 vers RJ-12). Si vous avez besoin de séparateurs ou de prises spéciales, prenez contact avec votre fournisseur d'accès.

3. Reliez une extrémité d'un câble réseau Ethernet à l'un des ports Ethernet (numérotés de 1 à 4) situés sur le panneau arrière du modem routeur et l'autre extrémité au port Ethernet d'un ordinateur.

   Procédez de même pour relier d'autres ordinateurs, un commutateur ou des périphériques réseau au modem routeur.

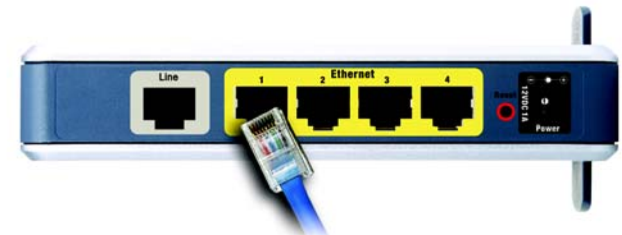


Figure 4-2 : Connexion d'un ordinateur

4. Connectez l'adaptateur électrique fourni au port Power (Alimentation) du modem routeur, puis branchez-le sur une prise d'alimentation.



REMARQUE : Branchez toujours l'adaptateur électrique du modem routeur sur une barrette de connexion protégée contre les surtensions.

Le voyant d'alimentation (Power) situé sur le panneau avant s'illumine en vert dès que l'adaptateur électrique est correctement connecté. Le voyant d'alimentation clignote pendant quelques secondes puis reste allumé une fois le test d'autodiagnostic terminé. Si le voyant clignote pendant au moins une minute, reportez-vous à l'« Annexe A : Dépannage ».



Figure 4-3 : Connexion de l'alimentation

5. Allumez un des ordinateurs connectés au modem routeur.

Passez au « Chapitre 5 : Configuration du modem routeur ADSL résidentiel sans fil G ».

Connexion sans fil à un ordinateur

Si vous souhaitez utiliser une connexion sans fil pour accéder au modem routeur, procédez comme suit :

1. Vérifiez que tous les appareils du réseau sont hors tension, y compris le modem routeur et tous les ordinateurs.

2. Branchez un câble téléphonique entre le port Line (Ligne) du panneau arrière du modem routeur et la prise murale de la ligne ADSL Il peut être nécessaire de placer un petit périphérique appelé microfiltre (non fourni) entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.



REMARQUE : Il peut être nécessaire de placer un petit périphérique appelé microfiltre (non fourni) entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.



IMPORTANT : Dans les pays où les prises téléphoniques sont utilisées avec des connecteurs RJ-11, veillez à placer les microfiltres entre le téléphone et la prise murale et **non pas** entre le modem routeur et la prise murale. Sinon, la connexion ADSL ne pourra pas être établie.

Dans les pays où les prises téléphoniques **ne sont pas** utilisées avec des connecteurs RJ-11 (par exemple, France, Suède, Suisse, Royaume-Uni, etc.), sauf pour les utilisateurs RNIS, le microfiltre doit être placé entre le modem routeur et la prise murale, car il contient le connecteur RJ-11.

Les utilisateurs de Annex B (versions E1 et DE du modem routeur) doivent utiliser le câble spécial fourni pour connecter le modem routeur à la prise murale (RJ-45 vers RJ-12). Si vous avez besoin de séparateurs ou de prises spéciales, prenez contact avec votre fournisseur d'accès.

3. Connectez l'adaptateur électrique fourni au port Power (Alimentation), puis branchez-le sur une prise d'alimentation.

   Le voyant d'alimentation (Power) situé sur le panneau avant s'illumine en vert dès que l'adaptateur électrique est correctement connecté. Le voyant d'alimentation clignote pendant quelques secondes puis reste allumé une fois le test d'autodiagnostic terminé. Si le voyant clignote pendant au moins une minute, reportez-vous à l'« Annexe A : Dépannage ».

4. Allumez un des ordinateurs de votre/vos réseau(x) sans fil.

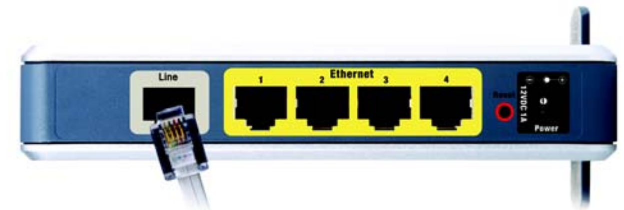


Figure 4-4 : Connexion d'une ligne ADSL



Figure 4-5 : Connexion de l'alimentation



REMARQUE : Veillez à toujours modifier le paramètre par défaut, **linksys**, et activer la sécurité sans fil.

5. Pour accéder initialement au modem routeur via une connexion sans fil, assurez-vous que le SSID de l'adaptateur sans fil est défini sur « **linksys** » (paramètre par défaut du modem routeur) et que sa fonction de sécurité sans fil est désactivée. Après que vous avez accédé au modem routeur, vous pouvez modifier les paramètres du modem routeur et de l'adaptateur de cet ordinateur pour qu'ils correspondent à vos paramètres réseau habituels.

Passez au « Chapitre 5 : Configuration du modem routeur ADSL résidentiel sans fil G ».

Chapitre 5 : Configuration du modem routeur ADSL résidentiel sans fil G

Présentation

Suivez les étapes contenues dans ce chapitre et configurez le modem routeur en utilisant son utilitaire Web. Ce chapitre décrit les pages Web de l'utilitaire ainsi que leurs fonctions clés. Vous pouvez accéder à l'utilitaire à partir de votre navigateur Web par l'intermédiaire d'un ordinateur connecté au modem routeur. Dans le cadre d'une configuration réseau de base, la plupart des utilisateurs pourront effectuer leurs opérations uniquement à partir des écrans de l'utilitaire suivants :

- Basic Setup (Configuration de base). Dans l'écran Basic Setup (Configuration de base), entrez les paramètres fournis par votre fournisseur d'accès Internet (FAI).
- Gestion. Cliquez sur l'onglet **Administration**, puis sur l'onglet **Management** (Gestion). Le nom d'utilisateur et le mot de passe par défaut du modem routeur est admin. Pour sécuriser le modem routeur, choisissez un mot de passe autre que le mot de passe par défaut.

Il existe sept onglets principaux : Setup (Configuration), Wireless (Sans fil), Security (Sécurité), Access Restrictions (Restrictions d'accès), Applications & Gaming (Applications et jeux), Administration et Status (Etat). D'autres onglets apparaissent lorsque vous cliquez sur les onglets principaux.

Configuration

- Basic Setup (Configuration de base). Entrez les paramètres de connexion Internet et de réseau dans cet écran.
- DDNS. Pour activer la fonctionnalité DDNS (Dynamic Domain Name System) du modem routeur, renseignez les champs à l'écran.
- Advanced Routing (Routage avancé). Dans cet écran, vous pouvez configurer les options NAT et de routage.

Sans fil

- (Basic Wireless Settings) Paramètres sans fil de base. Dans cet écran, vous pouvez sélectionner les paramètres de réseau sans fil.
- Wireless Security (Sécurité sans fil). Dans cet écran, vous pouvez configurer les paramètres de sécurité sans fil.
- Accès sans fil. Dans cet écran, vous pouvez contrôler l'accès à votre réseau sans fil.
- Advanced Wireless Settings (Paramètres sans fil avancés). Dans cet écran, vous pouvez accéder aux paramètres de réseau sans fil avancés.



AVEZ-VOUS : Avez-vous activé TCP/IP sur vos ordinateurs ? Les ordinateurs utilisent ce protocole pour communiquer sur le réseau. Pour obtenir plus d'informations sur TCP/IP, consultez l'aide de Windows.



REMARQUE : Pour plus de sécurité, modifiez votre mot de passe à partir de l'onglet Administration.

Sécurité

Dans cet écran, vous pouvez activer ou désactiver le pare-feu, définir des filtres, bloquer des requêtes WAN et activer ou désactiver l'option VPN PassThrough (Intercommunication VPN).

***vpn** (virtual private network) : mesure de sécurité visant à protéger des données lorsqu'elles quittent un réseau et s'acheminent vers un autre via Internet.*

Restrictions d'accès

- Internet Access (Accès Internet). Dans cet écran, vous pouvez contrôler l'exploitation et le trafic Internet de votre réseau local.

Applications et jeux

- Single Port Forwarding (Transfert de connexion unique). Dans cet écran, vous pouvez définir des services ou des applications fréquemment utilisés qui exigent un transfert de connexion unique.
- Port Range Forwarding (Transfert de connexion). Dans cet écran, vous pouvez définir des services publics ou autres applications Internet spécialisées qui exigent le transfert d'une série de connexions.
- Port Triggering (Déclenchement de connexion). Cet onglet vous permet de configurer des connexions déclenchées et des connexions transférées pour des applications Internet.
- DMZ. Cet écran vous permet d'autoriser l'exposition à Internet d'un ordinateur local, pour l'accès à des services spécifiques.
- QS (qualité de service). Utilisez la Qualité de service (QS) pour attribuer différents degrés de priorité à différents types de transmissions de données.

Administration

- Gestion. Cet écran vous permet de modifier les paramètres de gestion d'accès au modem routeur, SNMP (Simple Network Management Protocol), UPnP (Universal Plug and Play), proxy IGMP (Internet Group Multicast Protocol) et sans fil.
- Reporting (Rapports). Cet onglet vous permet de visualiser ou d'enregistrer des fichiers journaux d'activités.
- Diagnostics. Cet écran vous permet d'effectuer un test Ping.
- Backup&Restore (Sauvegarde&restauration). Cet écran vous permet de sauvegarder ou restaurer la configuration du modem routeur.
- Factory Defaults (Paramètres d'usine). Cet écran vous permet de restaurer les paramètres d'usine (par défaut) du modem routeur.
- Firmware Upgrade (Mise à jour du micrologiciel). Cet onglet vous permet de mettre à niveau le micrologiciel du modem routeur.
- Reboot (Redémarrage). Cet écran permet d'effectuer un redémarrage logiciel ou matériel du modem routeur.

Etat

- Gateway (Modem routeur). Cet écran contient des informations sur l'état du modem routeur.
- Local Network (Réseau local). Cet écran contient des informations sur l'état du réseau local.
- Wireless (Sans fil). Cet écran contient des informations sur l'état du réseau sans fil.
- DSL Connection (Connexion DSL). Cet écran contient des informations sur l'état de la connexion DSL.

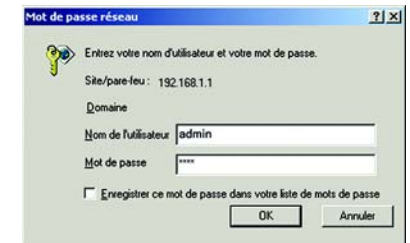


Figure 5-1 : Ecran Connexion

Comment accéder à l'utilitaire Web ?

Pour accéder à l'utilitaire Web, démarrez Internet Explorer ou Netscape Navigator, puis entrez l'adresse IP de passerelle par défaut, **192.168.1.1**, dans le champ *Address* (Adresse). Appuyez ensuite sur la touche **Entrée**.

Un écran de connexion apparaît (les utilisateurs de Windows XP voient apparaître un écran semblable). Saisissez **admin** (nom d'utilisateur par défaut) dans le champ *Nom d'utilisateur* et **admin** (mot de passe par défaut) dans le champ *Mot de passe*. Cliquez sur le bouton **OK**.

Onglet Setup (Configuration)

Onglet Basic Setup (Configuration de base)

Le premier écran qui s'affiche est l'onglet Basic Setup (Configuration de base). Les options de cet onglet vous permettent de modifier les paramètres généraux du modem routeur. Modifiez ces paramètres comme décrit ici et cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications, ou sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Internet Setup (Configuration Internet)

- Internet Connection Type (Type de connexion Internet). Le modem routeur prend en charge cinq méthodes d'encapsulation : RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA et Bridged Mode Only (Bridged Mode uniquement). Sélectionnez le type d'encapsulation qui convient dans le menu déroulant. Les écrans *Basic Setup* (Configuration de base) et les options disponibles varient selon le type d'encapsulation sélectionné.

- VC Settings (Paramètres VC). Cette section permet de configurer les paramètres VC.
  - Multiplexing (Multiplexage) : Sélectionnez **LLC** ou **VC** en fonction de votre FAI.
  - QoS Type (Type QS) : Sélectionnez une option dans le menu déroulant : **CBR** (Continuous Bit Rate) pour spécifier une bande passante fixe pour les transmissions vocales ou de données ; **UBR** (Unspecific Bit Rate) pour les applications qui ne sont pas sensibles au temps, comme la messagerie ; ou **VBR** (Variable Bite Rate) pour le trafic en rafales et le partage de bande passante avec d'autres applications.

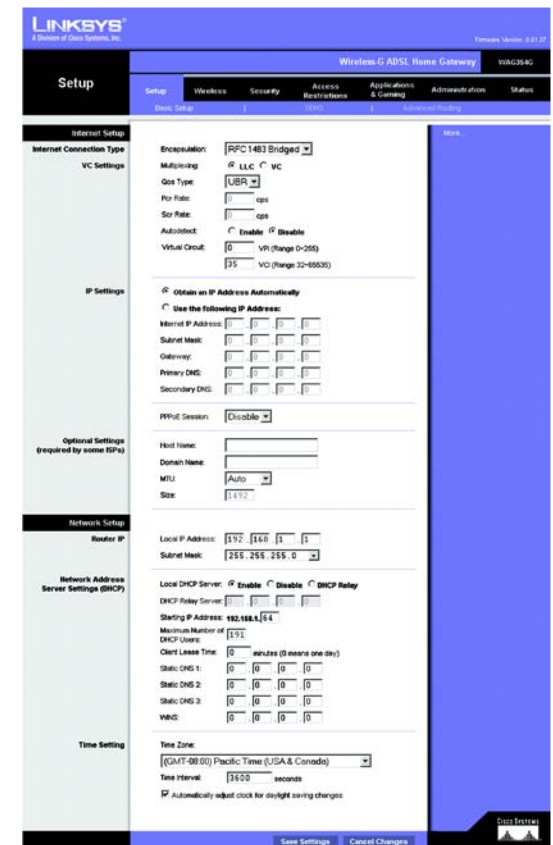


Figure 5-2 : Configuration de base

- Pcr Rate (Taux cr) : Pour calculer le taux cr, divisez le taux de la ligne DSL par 424. Vous obtenez le taux maximal d'envoi de cellules par l'expéditeur. Entrez le taux dans ce champ (s'il est requis par votre FAI).
- Scr Rate (Taux Scr) : Le taux Scr définit le taux moyen de cellules pouvant être transmises. Cette valeur est normalement inférieure au taux cr. Entrez le taux dans ce champ (s'il est requis par votre FAI).
- Autodetect (Détection automatique) : Sélectionnez **Enable** (Activer) pour que les paramètres soient entrés automatiquement ou **Disable** (Désactiver) pour entrer les valeurs manuellement.
- Virtual Circuit (Circuit virtuel) : Ces champs contiennent deux options : VPI (Virtual Path Identifier) et VCI (Virtual Channel Identifier). Votre FAI vous indiquera le paramétrage approprié de chacun de ces deux champs.

- Paramètres IP. Suivez les instructions de la section correspondant au type d'encapsulation choisi.

RFC 1483 Bridged

Adresse IP dynamique

Paramètres IP. Sélectionnez **Obtain an IP Address Automatically** (Obtenir une adresse IP automatiquement) si votre FAI vous indique que vous êtes connecté via une adresse IP dynamique.

Figure 5-3 : RFC 1483 Bridged - Adresse IP dynamique

IP statique

Si vous devez utiliser une adresse IP permanente (statique) pour vous connecter à Internet, sélectionnez **Use the following IP Address** (Utiliser l'adresse IP suivante).

- Internet IP Address (Adresse IP Internet). Il s'agit de l'adresse IP du modem routeur, vue par le WAN ou Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.
- Subnet Mask (Masque de sous-réseau). Il s'agit du masque de sous-réseau du modem routeur. Votre FAI peut vous fournir le masque de sous-réseau.
- Gateway (Passerelle) : Votre FAI peut vous fournir l'adresse de passerelle par défaut. Il s'agit en fait de l'adresse IP du serveur du FAI.
- Primary DNS (Nom de domaine primaire) (obligatoire) et Secondary DNS (Nom de domaine secondaire) (facultatif). Votre FAI peut vous fournir au moins une adresse IP de serveur DNS (Domain Name System).

Figure 5-4 : RFC 1483 Bridged - Adresse IP statique

RFC 1483 Routed

Si vous devez utiliser RFC 1483 Routed, sélectionnez **RFC 1483 Routed.**

- Internet IP Address (Adresse IP Internet). Il s'agit de l'adresse IP du modem routeur, vue par le WAN ou Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.
- Subnet Mask (Masque de sous-réseau). Il s'agit du masque de sous-réseau du modem routeur. Votre FAI peut vous fournir le masque de sous-réseau.
- Gateway (Passerelle) : Votre FAI peut vous fournir l'adresse de passerelle par défaut. Il s'agit en fait de l'adresse IP du serveur du FAI.
- Primary DNS (Nom de domaine primaire) (obligatoire) et Secondary DNS (Nom de domaine secondaire) (facultatif). Votre FAI peut vous fournir au moins une adresse IP de serveur DNS (Domain Name System).

Figure 5-5 : RFC 1483 Routed

RFC 2516 PPPoE

Certains fournisseurs d'accès Internet DSL utilisent le protocole PPPoE (protocole de point-à-point sur Ethernet) pour établir des connexions Internet. Si vous êtes connecté à Internet par l'intermédiaire d'une ligne DSL, demandez à votre FAI s'il utilise le protocole PPPoE. Si tel est le cas, vous devrez sélectionner l'option PPPoE.

- Service Name (Nom du service). Entrez le nom du service PPPoE dans le champ.
- User Name (Nom d'utilisateur) et Password (Mot de passe). Entrez le nom d'utilisateur et le mot de passe fournis par votre FAI.
- Connect on Demand (Connexion à la demande). Max Idle Time (Délai d'inactivité maximal). Vous pouvez configurer le modem routeur afin qu'elle désactive la connexion Internet après une période donnée d'inactivité. Si votre connexion Internet a été désactivée suite à son inactivité, l'option Connect on Demand (Connexion à la demande) permet au modem routeur de rétablir automatiquement votre connexion dès que vous tentez d'accéder de nouveau à Internet. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Connect on Demand (Connexion à la demande).** Dans le champ *Max Idle Time* (Délai d'inactivité maximal), entrez le nombre de minutes que vous souhaitez voir s'écouler avant la désactivation de votre connexion Internet.
- Keep Alive: Redial Period (Activée : Rappel après). Si vous sélectionnez cette option, le modem routeur procède régulièrement à une vérification de votre connexion Internet. Si vous êtes déconnecté, le modem routeur rétablit automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Keep Alive** (Activée). Dans le champ *Redial Period* (Rappel après), spécifiez la fréquence à laquelle le modem routeur doit vérifier votre connexion Internet. Le temps devant s'écouler par défaut avant rappel est de **20** secondes.

Figure 5-6 : RFC 2516 PPPoE

RFC 2364 PPPoA

Certains fournisseurs d'accès Internet (FAI) DSL utilisent le protocole PPPoA (protocole de point-à-point sur ATM) pour établir des connexions Internet. Si vous êtes connecté à Internet par l'intermédiaire d'une ligne DSL, demandez à votre FAI s'il utilise le protocole PPPoA. Si tel est le cas, vous devrez sélectionner l'option PPPoA.

- User Name (Nom d'utilisateur) et Password (Mot de passe). Entrez le nom d'utilisateur et le mot de passe fournis par votre FAI.
- Connect on Demand (Connexion à la demande). Max Idle Time (Délai d'inactivité maximal). Vous pouvez configurer le modem routeur afin qu'il désactive la connexion Internet après une période donnée d'inactivité. Si votre connexion Internet a été désactivée suite à son inactivité, l'option Connect on Demand (Connexion à la demande) permet au modem routeur de rétablir automatiquement votre connexion dès que vous tentez d'accéder de nouveau à Internet. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Connect on Demand** (Connexion à la demande). Dans le champ *Max Idle Time* (Délai d'inactivité maximal), entrez le nombre de minutes que vous souhaitez voir s'écouler avant la désactivation de votre connexion Internet.
- Keep Alive: Redial Period (Activée : Rappel après). Si vous sélectionnez cette option, le modem routeur procède régulièrement à une vérification de votre connexion Internet. Si vous êtes déconnecté, le modem routeur rétablit automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Keep Alive** (Activée). Dans le champ *Redial Period* (Rappel après), spécifiez la fréquence à laquelle le modem routeur doit vérifier votre connexion Internet. Le temps devant s'écouler par défaut avant rappel est de **20** secondes.

Figure 5-7 : RFC 2364 PPPoA

Bridged Mode Only (Bridged Mode uniquement)

Si vous utilisez votre modem routeur en tant que pont (elle fonctionne comme un modem autonome), sélectionnez **Bridged Mode Only** (Bridged Mode uniquement). Les paramètres NAT et de routage sont désactivés dans ce mode.

Optional Settings (Paramètres facultatifs) (Requis par certains FAI)

- Host Name (Nom d'hôte) et Domain Name (Nom de domaine). Entrez les noms d'hôte et de domaine du modem routeur dans ces deux champs. Certains FAI requièrent ces noms pour l'authentification. Vous devrez peut-être contacter votre FAI et vérifier si votre service Internet haut débit a été configuré avec un nom d'hôte et un nom de domaine. Dans la plupart des cas, vous pourrez laisser ces champs vides.
- MTU et Taille. Le paramètre MTU (Maximum Transmission Unit) spécifie la taille de paquet maximale autorisée pour la transmission réseau. Sélectionnez **Manual** (Manuel) et entrez la valeur souhaitée dans le champ *Size* (Taille). Il est recommandé d'entrer une valeur comprise entre 1200 et 1500. Par défaut, le paramètre MTU est configuré automatiquement.

Figure 5-8 : Bridged Mode Only (Bridged Mode uniquement)

Configuration réseau

- Router IP (Adresse IP du routeur). Les valeurs d'adresse IP locale et de masque de sous-réseau du modem routeur sont spécifiées dans ces champs. Dans la plupart des cas, il est recommandé de conserver les valeurs par défaut.
  - Local IP Address (Adresse IP locale). La valeur par défaut est **192.168.1.1**.
  - Subnet Mask (Masque de sous-réseau). La valeur par défaut est **255.255.255.0**.
- Network Address Server Settings (DHCP) (Paramètres du serveur d'adresse de réseau (DHCP)). Cette section permet de configurer les paramètres DHCP (Dynamic Host Configuration Protocol) du modem routeur.
  - Local DHCP Server (Serveur DHCP local). Un serveur Dynamic Host Configuration Protocol (DHCP) attribue automatiquement une adresse IP à chaque ordinateur du réseau. A moins que vous ne disposiez déjà d'un serveur DHCP, il est recommandé de laisser la fonction de serveur DHCP activée pour le modem routeur. Le modem routeur peut également être utilisée en mode Relais DHCP.
  - Serveur du relais DHCP Si vous activez le paramètre Relais DHCP du *serveur DHCP local*, entrez l'adresse IP du serveur DHCP dans les champs.
  - Starting IP Address (Adresse IP de départ). Entrez une valeur de départ pour la publication d'adresses IP sur le serveur DHCP. L'adresse IP de passerelle par défaut étant 192.168.1.1., cette valeur doit être égale à 192.168.1. 2 ou supérieure.
  - Maximum Number of DHCP Users (Nombre maximal d'utilisateurs DHCP). Entrez le nombre maximal d'utilisateurs/clients pouvant obtenir une adresse IP. Ce nombre varie en fonction de l'adresse IP de début spécifiée.
  - Client Lease Time (Durée de bail du client). Cette option détermine la période pendant laquelle un ordinateur est autorisé à se connecter au modem routeur à l'aide de son adresse IP dynamique actuelle. Entrez la durée (en minutes) pendant laquelle l'adresse IP dynamique est allouée à l'ordinateur.
  - Static DNS (DNS statique), 1 à 3. Le système DNS (Domain Name System) est le service adopté par Internet pour convertir des noms de domaine ou de site Web en adresses Internet ou URL. Votre FAI peut vous fournir au moins une adresse IP de serveur DNS. Vous pouvez taper jusqu'à trois adresses IP de serveur DNS. Le modem routeur utilise alors ces trois adresses IP pour accéder en un clin d'œil aux serveurs DNS en cours d'utilisation.
  - WINS. Le système WINS (Windows Internet Naming Service) convertit des noms NetBIOS en adresses IP. Si vous optez pour un serveur WINS, entrez son adresse IP dans ce champ. Autrement, laissez-le vide.
  - Time Setting (Réglage de l'heure). Sélectionnez le fuseau horaire correspondant à l'emplacement de votre modem routeur. Vous pouvez activer la case à cocher **Automatically adjust clock for daylight saving changes** (Régler automatiquement l'horloge en fonction des modifications de l'heure d'été).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Figure 5-9 : Paramètres facultatifs

Onglet DDNS

Le modem routeur inclut une fonction DDNS (Dynamic Domain Name System). vous permet d'attribuer un nom de domaine et d'hôte fixe à une adresse IP Internet dynamique. Cela peut s'avérer utile si vous hébergez votre propre site Web, un serveur FTP ou tout autre type de serveur derrière le modem routeur.

Avant d'opter pour cette fonctionnalité, vous devez obtenir la connexion à un service DDNS auprès de fournisseurs spécialisés, tels que DynDNS.org ou TZO.com.

DDNS

DDNS Service (Service DDNS). Si votre service DDNS est fourni par DynDNS.org, sélectionnez **DynDNS.org** dans le menu déroulant. Si votre service DDNS est fourni par DynDNS.org, sélectionnez **TZO.com** dans le menu déroulant. Pour désactiver le service DDNS, sélectionnez **Disabled** (Désactivé).

DynDNS.org

- User Name (Nom d'utilisateur), Password (Mot de passe) et Host Name (Nom d'hôte). Entrez le nom d'utilisateur, le mot de passe et le nom d'hôte du compte configuré avec DynDNS.org.
- Internet IP Address (Adresse IP Internet). L'adresse IP Internet actuelle du modem routeur est spécifiée dans ce champ. Puisqu'elle est dynamique, cette adresse change.
- Status (Etat). L'état de la connexion du service DDNS est spécifié dans ce champ.

TZO.com

- Email Address (Adresse électronique), Password (Mot de passe) et Domain Name (Nom de domaine). Entrez l'adresse électronique, le mot de passe et le nom de domaine du compte configuré avec TZO.
- Internet IP Address (Adresse IP Internet). L'adresse IP Internet actuelle du modem routeur est spécifiée dans ce champ. Puisqu'elle est dynamique, cette adresse change.
- Status (Etat). L'état de la connexion du service DDNS est spécifié dans ce champ.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.



Figure 5-10 : DynDNS.org



Figure 5-11 : TZO.com

Onglet Advanced Routing (Routage avancé)

L'écran *Advanced Routing* (Routage avancé) vous permet de configurer les paramètres NAT, de routage dynamique et de routage statique.

Advanced Routing (Routage avancé)

- Operating Mode (Mode opérationnel). Cette section permet de configurer les paramètres de routage généraux du modem routeur.
  - NAT. NAT est une fonction de sécurité activée par défaut. Elle permet au modem routeur de convertir les adresses IP d'un réseau local en une adresse IP distincte sur Internet. Pour désactiver NAT, cliquez sur le bouton d'option **Disabled** (Désactivé).
  - RIP. Si votre réseau comporte plusieurs routeurs, vous pouvez utiliser le protocole RIP (Routing Information Protocol) de façon à ce que les routeurs échangent des informations de routage. Pour utiliser le protocole RIP, sélectionnez le bouton radio **Enabled** (Activé). Sinon, conservez la valeur par défaut, **Disabled** (Désactivé).
  - Envoyer itinéraire par défaut. Pour utiliser la version de routage RIP 1, sélectionnez le bouton radio **Enabled** (Activé). Sinon, conservez la valeur par défaut, **Disabled** (Désactivé).
  - Interface (Interface). Ce paramètre est disponible si vous avez configuré un itinéraire statique et que vous devez choisir une interface pour cet itinéraire. Sélectionnez l'interface utilisée par le modem routeur : **LAN/Wireless** (LAN/Sans fil) ou **Internet.**
- Dynamic Routing (Routage dynamique). Le routage dynamique vous permet d'exiger du modem routeur qu'elle s'adapte aux modifications physiques de la configuration du réseau. Le modem routeur, à l'aide du protocole RIP, détermine l'itinéraire des paquets du réseau en fonction du plus petit nombre de sauts relevés entre la source et la destination. Le protocole RIP transmet régulièrement les informations de routage aux autres modems routeurs du réseau.
  - Version de transmission RIP. Pour transmettre des messages RIP, sélectionnez le protocole souhaité : **RIP1, RIP1-Compatible** (Compatible RIP1) ou **RIP2.** Si vous ne voulez pas transmettre de messages RIP, sélectionnez **None** (Aucun).
  - Receive RIP Version (Version de réception RIP). Pour recevoir des messages RIP, sélectionnez le protocole souhaité : **RIP1** ou **RIP2.** Si vous ne voulez pas recevoir de messages RIP, sélectionnez **None** (Aucun).

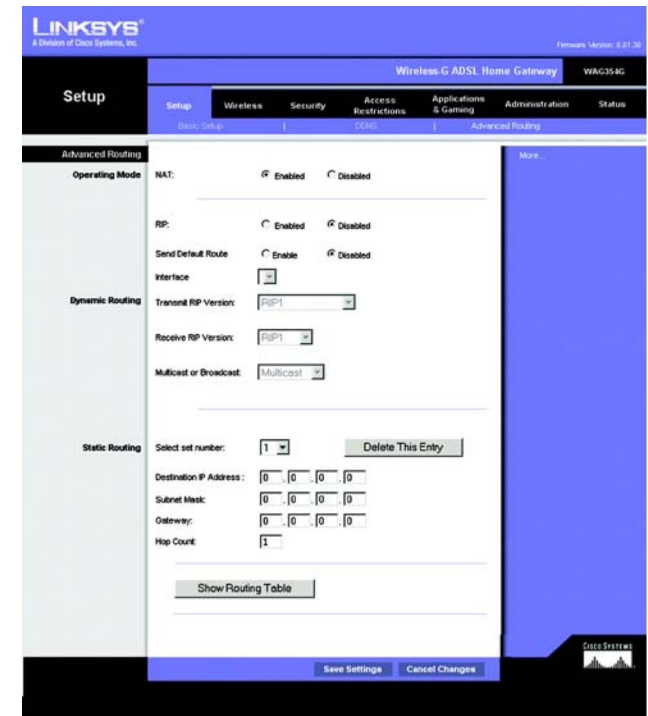


Figure 5-12 : Advanced Routing (Routage avancé)

- Multicast (Multidiffusion) ou Broadcast (Diffusion). Les messages RIP peuvent être envoyés à l'aide des deux méthodes. Si vous souhaitez utiliser la multidiffusion, sélectionnez **Multicast** (Multidiffusion) Si vous souhaitez utiliser la diffusion, sélectionnez **Broadcast** (Diffusion).

- Static Routing (Routage statique). Si le modem routeur est connectée à plusieurs réseaux, il peut être nécessaire de définir un itinéraire statique entre eux. Un itinéraire statique est une voie prédéfinie que les informations du réseau doivent emprunter pour atteindre un hôte ou un réseau spécifique. Pour créer un itinéraire statique, modifiez les paramètres suivants :

  - Sélectionner le numéro de jeu (set number). Sélectionnez le numéro de l'itinéraire statique dans le menu déroulant. Le modem routeur peut prendre en charge jusqu'à 20 entrées d'itinéraires statiques. Si vous souhaitez supprimer un itinéraire, une fois l'entrée sélectionnée, cliquez sur le bouton **Delete This Entry** (Supprimer cette entrée).

  - Destination IP Address (Adresse IP de destination). Cette option identifie l'adresse du réseau distant, ou hôte, auquel vous souhaitez attribuer un itinéraire statique. Entrez l'adresse IP de l'hôte pour lequel vous souhaitez créer un itinéraire statique. Si vous créez un itinéraire pour l'intégralité du réseau, assurez-vous que la portion de réseau de l'adresse IP est définie sur 0.

  - Subnet Mask (Masque de sous-réseau). Entrez le masque de sous-réseau (également appelé Masque de réseau), qui détermine la portion de l'adresse IP qui correspond au réseau et la portion de l'adresse IP qui correspond à l'hôte.

  - Gateway (Passerelle) : Entrez l'adresse IP du périphérique qui permet le contact entre le modem routeur et le réseau distant ou hôte.

  - Hop Count (Nombre de sauts). Il s'agit du nombre de sauts entre un noeud et la destination (16 tronçons au maximum). Entrez le nombre de sauts dans ce champ.

- Show Routing Table (Afficher la table de routage). Cliquez sur le bouton **Show Routing Table** (Afficher la table de routage) pour afficher un écran indiquant l'itinéraire des données sur le réseau local. Pour chaque itinéraire, l'adresse IP du réseau local de destination, le masque de sous-réseau, le modem routeur et l'interface sont affichés. Cliquez sur le bouton **Refresh** (Actualiser) pour mettre à jour les informations. Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran précédent.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Routing Table Entry List

Refresh

Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	LAN & Wireless

Close

Figure 5-13 : Routing Table (Table de routage)

Onglet Wireless (Sans fil)

Onglet Basic Wireless Settings (Paramètres sans fil de base)

Cet écran vous permet de sélectionner votre mode réseau sans fil ainsi que votre sécurité sans fil.

Wireless Network (Réseau sans fil)

- Wireless Network Mode (Mode réseau sans fil). Si votre réseau comporte des périphériques 802,11g et 802,11b, conservez le paramètre par défaut, **Mixed** (Mixte). Si votre réseau comporte uniquement des périphériques 802,11g, sélectionnez **802,11g**. S'il comporte uniquement des périphériques 802,11b sélectionnez **802,11b**. Si vous souhaitez désactiver la mise en réseau sans fil, sélectionnez **Disabled** (Désactivé).

- Wireless Network Name (SSID) (Nom du réseau sans fil (SSID)). Entrez le nom de votre réseau sans fil dans ce champ. Il s'agit du nom de réseau que partagent tous les périphériques interconnectés à un réseau sans fil. Il doit être identique pour tous les périphériques du réseau sans fil. Ce paramètre est sensible à la casse et ne doit pas comprendre plus de 32 caractères alphanumériques. Tous les caractères du clavier peuvent être utilisés. Linksys vous recommande de remplacer le nom SSID par défaut (linksys) par un nom unique de votre choix.

- Wireless Channel (Canal sans fil). Sélectionnez le canal approprié dans la liste fournie en fonction de vos paramètres réseau. Tous les points de votre réseau sans fil doivent utiliser le même canal pour fonctionner correctement. Les ordinateurs ou clients sans fil détecteront automatiquement le canal sans fil du modem routeur.

- Wireless SSID Broadcast (Diffusion SSID sans fil). Lorsque des ordinateurs ou des clients sans fil recherchent sur le réseau local des réseaux sans fil auxquels s'associer, ils détectent le SSID diffusé par le modem routeur. Pour diffuser le SSID du modem routeur, conservez le paramètre par défaut, **Enable** (Activer). Si vous ne souhaitez pas diffuser le SSID du modem routeur, sélectionnez **Disable** (Désactiver).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

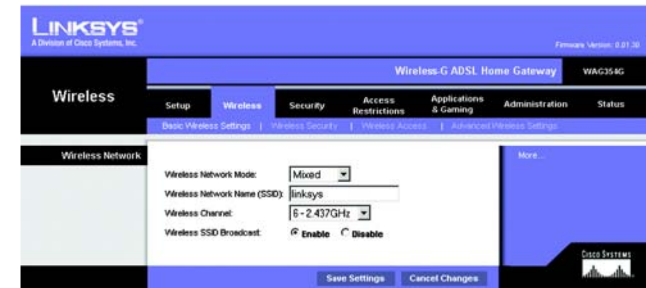


Figure 5-14 : Paramètres sans fil de base

Onglet Wireless Security (Sécurité sans fil)

Les paramètres de cette section permettent de configurer la sécurité de votre réseau sans fil. Le modem routeur prend en charge deux options de sécurité sans fil : WPA Pre-Shared Key (Clé WPA pré partagée) et WEP. WPA, acronyme de Wi-Fi Protected Access, désigne une norme de sécurité plus puissante que le système de cryptage WEP. WEP est l'acronyme de Wired Equivalent Privacy. Ces deux options font l'objet d'une description sommaire ci-après. Pour obtenir des instructions plus détaillées sur la configuration de la sécurité sans fil du modem routeur, consultez « l'annexe B : Sécurité sans fil ». Si vous souhaitez désactiver la sécurité sans fil, sélectionnez **Disable** (Désactiver) dans le menu déroulant du mode de sécurité.

WPA Pre-Shared Key (Clé WPA prépartagée). Entrez une clé partagée WPA composée de 8 à 32 caractères. Renseignez ensuite le champ Group Key Renewal (Renouvellement des clés du groupe) pour indiquer au modem routeur la fréquence à laquelle elle doit changer les clés de cryptage.



Figure 5-15 : Clé WPA pré partagée

WEP. Le système WEP est une méthode de cryptage de base qui n'est pas aussi sûre que le système WPA. Pour utiliser ce système, sélectionnez une clé par défaut (indique la clé à utiliser) puis un niveau de cryptage WEP : **64 bits et 10 chiffres hexadécimaux** ou **128 bits et 26 chiffres hexadécimaux**. Générez ensuite une clé WEP à partir de l'option Passphrase (Phrase mot de passe) ou entrez-la manuellement.

- WEP Encryption (Cryptage WEP) : Acronyme de Wired Equivalent Privacy, le WEP est une méthode de cryptage utilisée pour protéger vos communications sans fil. Le WEP utilise des clés 64 bits ou 128 bits pour contrôler l'accès à votre réseau et assurer la sécurité par le cryptage de chaque transmission de données. Pour décoder les données transmises, tous les périphériques d'un réseau doivent utiliser une clé WEP identique. Des niveaux de cryptage supérieurs offrent des niveaux de sécurité supérieurs mais, en raison de la complexité du cryptage, ils peuvent également diminuer les performances du réseau. Pour activer le cryptage WEP, sélectionnez **64 bits 10 hex digits** (64 bits 10 chiffres hexadécimaux) ou **128 bits 26 hex digits** (128 bits 26 chiffres hexadécimaux).

- Default Transmit Key (Clé de transmission par défaut). Sélectionnez la clé WEP (1-4) que vous souhaitez utiliser lorsque le modem routeur transmet des données. Assurez-vous que le périphérique récepteur (ordinateur ou client sans fil) utilise la même clé.

- Passphrase (Phrase mot de passe). Au lieu d'entrer manuellement les clés WEP, vous pouvez entrer une phrase mot de passe. Cette phrase mot de passe permet de générer une ou plusieurs clés WEP. Ce paramètre sensible à la casse ne doit pas comporter plus de 32 caractères alphanumériques. Cette fonction est compatible avec les produits sans fil Linksys uniquement et ne peut pas être utilisée avec l'utilitaire de configuration automatique de réseau sans fil de Windows XP. Si vous souhaitez communiquer avec des produits sans fil autres que des produits Linksys ou avec l'utilitaire de configuration automatique de réseau sans fil de Windows XP, notez la clé WEP générée dans le champ WEP *Key 1* (Clé WEP 1) et entrez-la manuellement dans l'ordinateur ou le client sans fil. Une fois la phrase mot de passe saisie, cliquez sur le bouton **Generate** (Générer) pour créer les clés WEP.

- WEP Keys 1-4 (Clés WEP 1-4). Les clés WEP vous permettent de créer un schéma de cryptage pour les transmissions réseau sans fil. Si vous n'utilisez pas de phrase mot de passe, entrez manuellement un ensemble de valeurs. Ne laissez aucun champ vierge et n'entrez pas de zéro, ce ne sont pas des valeurs de clés valides. Si vous utilisez un cryptage WEP 64 bits, la clé doit être constituée de 10 caractères hexadécimaux exactement. Si vous utilisez un cryptage WEP 128 bits, la clé doit être constituée de 26 caractères hexadécimaux exactement. Les caractères hexadécimaux valides sont : « 0 à 9 » et « A à F ».

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour obtenir des instructions plus détaillées sur la configuration de la sécurité sans fil du modem routeur, consultez « l'annexe B : Sécurité sans fil ».



Figure 5-16 : WEP

Onglet Wireless Access (Accès sans fil)

Wireless Network Access (Accès réseau sans fil)

Wireless Network Access (Accès réseau sans fil). Sélectionnez **Allow All** (Tout autoriser), si vous souhaitez autoriser tous les ordinateurs à accéder au réseau sans fil. Pour restreindre l'accès au réseau, sélectionnez **Restrict Access** (Restreindre l'accès), puis sélectionnez **Prevent** (Interdire) pour interdire l'accès aux ordinateurs désignés ou **Permit only** (Autoriser uniquement) pour autoriser l'accès des ordinateurs désignés. Cliquez sur le bouton **Edit MAC Address Access List** (Modifier la liste de filtrage des adresses MAC) ; l'écran the *Mac Address Filter List* (Liste de filtrage des adresses MAC) s'affiche.

Entrez les adresses MAC des ordinateurs que vous souhaitez désigner. Pour consulter une liste d'adresses MAC d'ordinateurs ou de clients sans fil, cliquez sur le bouton **Wireless Client MAC List** (Liste MAC des clients sans fil).

L'écran *Wireless Client MAC List* (Liste MAC des clients sans fil) dresse la liste des ordinateurs, de leurs adresses IP et de leurs adresses MAC. Cliquez sur le bouton Refresh (Actualiser) pour afficher les informations les plus récentes. Cliquez sur la case à cocher **Enable MAC Filter** (Activer le filtre MAC) pour ajouter un ordinateur spécifique à la liste de filtrage des adresses MAC ; cliquez sur la case à cocher **Enable MAC Filter** (Activer le filtre MAC) puis sur le bouton **Update Filter List** (Mettre à jour la liste des filtres). Cliquez sur le bouton **Close** (Fermer) pour revenir vers l'écran *Wireless Client MAC List* (Liste MAC des clients sans fil).

Sur l'écran *Wireless Client MAC List* (Liste MAC des clients sans fil), cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer la liste ou sur le bouton **Cancel Changes** (Annuler les modifications) pour les supprimer.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

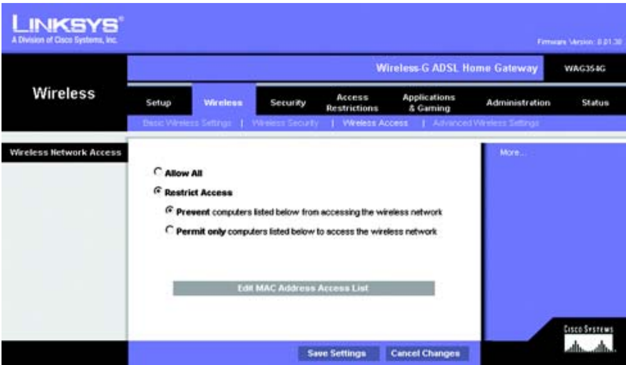


Figure 5-17 : Wireless Network Access (Accès réseau sans fil)

MAC Address Filter List

Enter MAC Address Format: xxxxxxxxxxxx/xx:xx:xx:xx:xx:xx

MAC 01: MAC 02: MAC 03: MAC 04: MAC 05: MAC 06: MAC 07: MAC 08: MAC 09: MAC 10:

MAC 11: MAC 12: MAC 13: MAC 14: MAC 15: MAC 16: MAC 17: MAC 18: MAC 19: MAC 20:

Wireless Client MAC List

Save Settings Cancel Changes

Figure 5-18 : Liste de filtrage des adresses MAC

Wireless Client MAC List Refresh

Computer Name	IP Address	MAC Address	Enable MAC Filter

Update Filter List Close

Figure 5-19 : Liste MAC des clients sans fil

Onglet Advanced Wireless Settings (Paramètres sans fil avancés)

Advanced Wireless (Paramètres sans fil avancés)

Cet écran vous permet d'accéder aux paramètres sans fil avancés suivants : Authentication Type (Type d'authentification), Control Tx Rates (Débits Tx de contrôle), Beacon Interval (Intervalle de transmission de balise), DTIM Interval (Intervalle DTIM), Fragmentation Threshold (Seuil de fragmentation) et RTS Threshold (Seuil RTS).

- Authentication Type (Type d'authentification) La valeur **Auto** définie par défaut vous permet de choisir entre une authentification Open System (Ouvert) ou Shared Key (Partagé). En mode d'authentification Système ouvert, l'expéditeur et le destinataire n'utilisent pas de clé WEP pour l'authentification mais peuvent utiliser le WEP pour le cryptage des données. Pour autoriser uniquement une authentification Open System (Système ouvert), sélectionnez **Open System** (Système ouvert). Pour l'authentification Clé partagée, l'expéditeur et le destinataire utilisent une clé WEP pour l'authentification et le cryptage des données. Pour autoriser uniquement une authentification Shared Key (Clé partagée), sélectionnez **Shared Key** (Clé partagée). Il est recommandé de conserver cette option en mode par défaut (Auto), car certains clients ne peuvent pas être configurés pour l'authentification Clé partagée.
- Control Tx Rates (Débits Tx de contrôle). Le débit de transmission par défaut est **Auto**. Vous devez définir le taux en fonction de la vitesse de votre réseau sans fil. Vous pouvez faire votre choix parmi les diverses vitesses de transmission proposées ou sélectionner l'option par défaut **Auto** pour demander au modem routeur d'adopter automatiquement le taux de transmission le plus rapide possible et activer la fonctionnalité de reconnexion automatique. Cette fonctionnalité est alors chargée de définir la meilleure vitesse de connexion possible entre le modem routeur et un client sans fil.
- Beacon Interval (Intervalle de transmission de balise). La valeur par défaut est **100.** La valeur Intervalle de transmission de balise indique l'intervalle de fréquence de la balise. Une balise désigne un paquet diffusé par le modem routeur pour synchroniser le réseau sans fil.
- DTIM Interval (Intervalle DTIM). La valeur par défaut est **1.** Cette valeur indique l'intervalle du message d'indication de transmission de données (DTIM). Un champ DTIM est un champ de compte à rebours chargé d'informer les clients sur la prochaine fenêtre à utiliser pour écouter des messages de diffusion ou de multidiffusion. Après avoir mis en mémoire tampon les messages de diffusion ou de multidiffusion des clients qui lui sont associés, le modem routeur transmet le DTIM suivant avec une valeur d'intervalle DTIM. Ses clients sont informés par les balises et se préparent à recevoir les messages de diffusion et de multidiffusion.
- Fragmentation Threshold (Seuil de fragmentation). Il est préférable de conserver la valeur par défaut de **2346.** Cette valeur permet de spécifier la taille maximale d'un paquet avant de fragmenter les données en plusieurs paquets. Si le taux d'erreur de paquet que vous rencontrez est élevé, vous pouvez légèrement augmenter le seuil de fragmentation. Un seuil de fragmentation trop bas peut se traduire par des performances faibles du réseau. Seule une petite modification de cette valeur est recommandée.
- RTS Threshold (Seuil RTS). Il est préférable de conserver la valeur par défaut de **2347.** Si vous faites face à un flux de données incohérent, seule une modification légère de la valeur est recommandée. Si un paquet du réseau apparaît plus petit que la taille prédéfinie du seuil RTS, le mécanisme RTS/CTS n'est pas activé. Le modem routeur transmet des trames RTS (Request To Send, demande d'émission) à une station de réception donnée et négocie l'envoi d'une trame de données. Après réception d'un signal RTS, la station sans fil répond par une trame CTS (Clear To Send, prêt à émettre) pour autoriser le début de la transmission.



Figure 5-20 : Advanced Wireless Settings (Paramètres sans fil avancés)

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Onglet Security (Sécurité)

Cet écran affiche les paramètres d'intercommunication VPN, de pare-feu et de filtre. Ces fonctions permettent d'améliorer la sécurité du réseau.

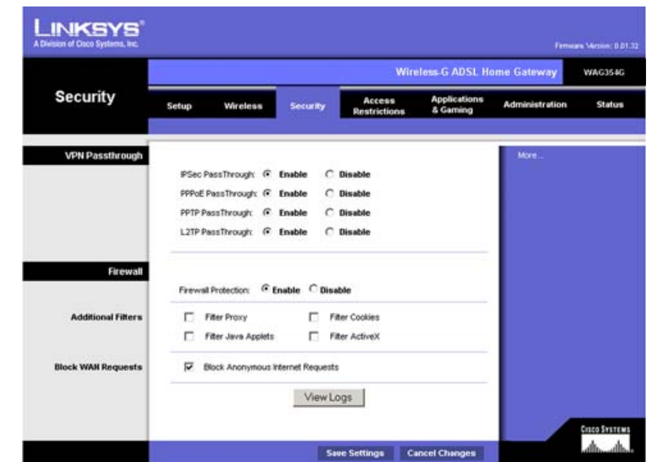


Figure 5-21 : Sécurité

VPN Passthrough (Intercommunication VPN)

VPN (Virtual Private Networking) est une mesure de sécurité qui crée une connexion sécurisée entre deux emplacements distants. Si vous configurez ces paramètres, le modem routeur autorisera le passage de tunnels VPN.

- IPSec Passthrough (Intercommunication IPSec). La technologie IPSec (Internet Protocol Security) désigne une série de protocoles utilisés pour la mise en place d'un échange sécurisé des paquets au niveau de la couche IP. Pour activer l'option Intercommunication IPSec, cliquez sur le bouton **Enable** (Activée). Pour désactiver l'option Intercommunication IPSec, cliquez sur le bouton **Disable** (Désactivée).
- Intercommunication PPPoE. L'option Intercommunication PPPoE vous permet d'utiliser le logiciel client PPPoE fourni par votre FAI sur votre(vos) ordinateur(s). Certains FAI exigent que cette fonction soit utilisée sur le modem routeur. Pour activer l'option Intercommunication PPPoE, cliquez sur le bouton **Enable** (Activer). Pour désactiver l'option Intercommunication PPPoE, cliquez sur le bouton **Disable** (Désactiver).
- PPTP Passthrough (Intercommunication PPTP). L'intercommunication PPTP (Point-to-Point Tunneling Protocol) est la méthode utilisée pour activer les sessions VPN dans un serveur Windows NT 4.0 ou 2000. Pour activer l'option Intercommunication PPTP, cliquez sur le bouton **Enable** (Activer). Pour désactiver l'option Intercommunication PPTP, cliquez sur le bouton **Disable** (Désactiver).
- L2TP Passthrough (Intercommunication L2TP). L'Intercommunication L2TP (Layer 2 Tunneling Protocol) est une extension de PPTP (Point-to-Point Tunneling Protocol) utilisée pour activer le fonctionnement d'un VPN sur Internet. Pour activer l'intercommunication L2TP, cliquez sur le bouton **Enable** (Activer). Pour désactiver l'option Intercommunication L2TP, cliquez sur le bouton **Disable** (Désactiver).

Firewall (Pare-feu)

Vous pouvez activer ou désactiver le pare-feu, définir des filtres pour bloquer des types de données Internet spécifiques et bloquer les requêtes Internet anonymes.

Pour utiliser le pare-feu, cliquez sur **Enable** (Activer). Si vous ne souhaitez pas l'utiliser, cliquez sur **Disable** (Désactiver).

Filtres supplémentaires

- Filter Proxy (Filtrer le proxy). L'utilisation de serveurs proxy WAN peut compromettre la sécurité du modem routeur. La suppression du filtre de proxy désactive l'accès aux serveurs de proxy WAN. Pour activer le filtre de proxy, sélectionnez la case à cocher.
- Filter Cookies (Filtrer les cookies). Un cookie est un ensemble de données stocké sur votre ordinateur et utilisé par les sites Internet lorsque vous consultez des pages Web. Pour activer le filtrage des cookies, sélectionnez la case à cocher.
- Filter Java Applets (Filtrer les Applets Java). Java est un langage de programmation pour sites Web. Si vous supprimez le filtrage des applets Java, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de programmation. Pour activer le filtrage des Applet Java, sélectionnez la case à cocher.
- Filter ActiveX (Filtrer ActiveX). ActiveX est un langage de programmation pour sites Web. Si vous supprimez le filtrage ActiveX, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de programmation. Pour activer le filtrage ActiveX, sélectionnez la case à cocher.

Blocage des requêtes WAN

- Block Anonymous Internet Requests (Bloquer les requêtes Internet anonymes). Cette option permet à votre réseau de ne pas être détecté et renforce votre sécurité en cachant vos ports réseau. Les intrus auront ainsi plus de difficultés à découvrir votre réseau. Sélectionnez l'option **Bloquer les requêtes Internet anonymes**. Pour autoriser ces requêtes, désélectionnez cette option**, désélectionnez cette option**.

Pour afficher les journaux d'activités des mesures de sécurité, cliquez sur le bouton **View Logs** (Afficher les fichiers journaux). Cliquez sur le bouton **Clear** (Supprimer) pour supprimer les informations. Cliquez sur le bouton **pageRefresh** (Actualiser la page) pour mettre à jour les informations. Cliquez sur le bouton **Previous Page** (Page précédente) pour revenir à la page précédente. Cliquez sur le bouton **Next Page** (Page suivante) pour accéder à la page suivante.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

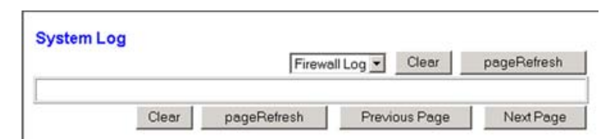


Figure 5-22 : Fichier journal du pare-feu

Onglet Access Restrictions (Restrictions d'accès)

Onglet Internet Access (Accès à Internet)

L'écran *Internet Access* (Accès Internet) vous permet de bloquer ou d'autoriser des modes spécifiques d'exploitation Internet. Vous pouvez définir vos stratégies d'accès à Internet pour des ordinateurs spécifiques et bloquer l'accès à certains sites Web avec leur URL ou leur mot de passe.

Internet Access Policy (Stratégie d'accès à Internet). Vous pouvez contrôler l'accès à l'aide d'une stratégie. Utilisez les paramètres de cet écran pour définir une stratégie d'accès (après avoir cliqué sur le bouton **Save Settings** (Enregistrer les paramètres)). La sélection d'une stratégie dans le menu déroulant permet d'afficher les paramètres de la stratégie en question. Pour supprimer une stratégie, sélectionnez son numéro, puis cliquez sur le bouton **Delete** (Supprimer). Pour afficher l'ensemble des stratégies, cliquez sur le bouton **Summary** (Récapitulatif). Vous pouvez supprimer les stratégies à partir de l'écran *Summary* (Récapitulatif) en sélectionnant la ou les stratégies, puis en cliquant sur le bouton **Delete** (Supprimer). Pour revenir à l'écran Internet Access (Accès à Internet), cliquez sur le bouton **Close** (Fermer).

Status (Etat) : Par défaut, les stratégies sont activées. Pour activer une stratégie, sélectionnez son numéro dans le menu déroulant, puis cliquez sur le bouton radio en regard de l'option *Enable* (Activer).

Pour créer une stratégie d'accès à Internet :

1. Sélectionnez un numéro dans le menu déroulant *Internet Access Policy* (Stratégie d'accès à Internet).

2. Pour activer cette stratégie, cliquez sur le bouton radio en regard de l'option *Enable* (Activer).

3. Entrez le nom de la stratégie dans le champ (Nom de la stratégie) Policy Name prévu à cet effet.

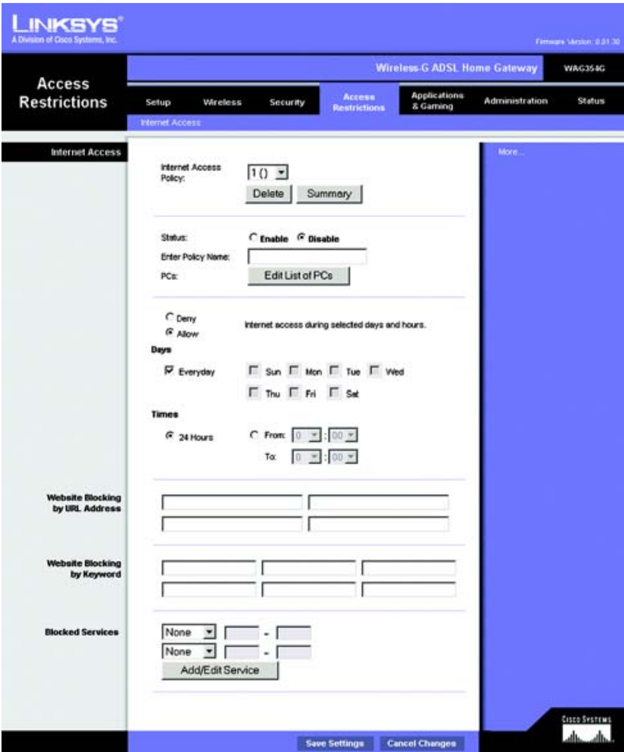


Figure 5-23 : Internet Access (Accès Internet)

Internet Policy Summary

No.	Policy Name	Days	Time of Day	Delete
1.	—	S M T W T F S	—	☐
2.	—	S M T W T F S	—	☐
3.	—	S M T W T F S	—	☐
4.	—	S M T W T F S	—	☐
5.	—	S M T W T F S	—	☐
6.	—	S M T W T F S	—	☐
7.	—	S M T W T F S	—	☐
8.	—	S M T W T F S	—	☐
9.	—	S M T W T F S	—	☐
10.	—	S M T W T F S	—	☐

Close

Figure 5-24 : Récapitulatif de la stratégie Internet

4. Cliquez sur le bouton **Edit List of PCs** (Liste des ordinateurs) pour sélectionner les ordinateurs auxquels cette stratégie doit s'appliquer. L'écran *List of PCs* (Liste des ordinateurs) apparaît. Vous pouvez sélectionner un ordinateur selon son adresse MAC ou son adresse IP. Vous pouvez également entrer une plage d'adresses IP si vous souhaitez appliquer cette stratégie à un groupe d'ordinateurs. Une fois vos modifications effectuées, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour valider ces modifications ou sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.
5. Sélectionnez l'option appropriée **Deny** (Refuser) ou **Allow** (Autoriser) selon ce que vous voulez faire, soit bloquer ou autoriser l'accès Internet aux ordinateurs répertoriés dans l'écran *List of PCs* (Lister des ordinateurs).
6. Définissez les jours et les heures pendant lesquels vous souhaitez appliquer cette stratégie. Sélectionnez individuellement les jours pendant lesquels la stratégie doit être en vigueur, ou bien sélectionnez l'option **Everyday** (Tous les jours). Entrez une plage d'heures et de minutes pendant laquelle la stratégie sera appliquée, ou bien sélectionnez l'option **24 Hours** (24 heures).
7. Si vous souhaitez bloquer des sites Web dotés d'adresses URL spécifiques, entrez chaque URL dans un champ distinct en regard de la section *Website Blocking by URL Address* (Blocage du site Web par adresse URL).
8. Si vous souhaitez bloquer des sites Web à l'aide de mots clés spécifiques, entrez chaque mot clé dans un champ distinct en regard de la section *Website Blocking by Keyword* (Blocage du site Web par mot clé).
9. Vous pouvez filtrer l'accès à divers services accessibles par Internet, notamment le service FTP ou Telnet, en choisissant ces services dans les menus déroulants en regard de l'option *Blocked Services* (Services bloqués).

   Entrez ensuite l'étendue des ports à filtrer.

   Si le service que vous envisagez de bloquer n'apparaît pas dans la liste ou si vous souhaitez modifier les paramètres d'un service, cliquez alors sur le bouton **Add/Edit Service** (Ajouter/Modifier un service). L'écran *Port Services* (Services des ports) apparaît.

   Pour ajouter un service, entrez son nom dans le champ *Service Name* (Nom du service). Sélectionnez son protocole dans le menu déroulant *Protocol* (Protocole), puis entrez son étendue dans les champs *Port Range* (Etendue des ports). Cliquez ensuite sur le bouton **Add** (Ajouter)

   Pour modifier un service, sélectionnez-le dans la liste de droite. Modifiez son nom, son paramètre de protocole ou l'étendue des ports. Cliquez ensuite sur le bouton **Modify** (Modifier).

   Pour supprimer un service, sélectionnez-le dans la liste de droite. Cliquez ensuite sur le bouton **Delete** (Supprimer).

   Une fois vos modifications dans l'écran *Port Services* (Services des ports) terminées, cliquez sur le bouton **Apply** (Appliquer) pour les enregistrer. Pour les annuler, cliquez sur le bouton **Cancel** (Annuler). Pour fermer l'écran *Port Services* (Services des ports) et revenir à l'écran *Access Restrictions* (Restrictions d'accès), cliquez sur le bouton **Close** (Fermer).
10. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer les paramètres de la stratégie. Pour annuler ces mêmes paramètres, cliquez sur le bouton **Cancel Changes** (Annuler les modifications).

Figure 5-25 : Liste des ordinateurs

Figure 5-26 : Ajouter/Modifier un service

Onglet Applications and Gaming (Applications et jeux)

Onglet Single Port Forwarding (Transfert de connexion unique)

Single Port Forwarding (Transfert de connexion unique)

L'écran *Single Port Forwarding* (Transfert de connexion unique) vous permet d'ouvrir un port spécifique de façon à ce que les utilisateurs puissent voir, sur Internet, les serveurs qui se trouvent derrière le modem routeur (tels que serveurs FTP ou de messagerie électronique). Lorsque des utilisateurs envoient ce type de requête vers votre réseau via Internet, le modem routeur transfère ces requêtes vers l'ordinateur approprié. Tout ordinateur dont le port est transféré doit avoir sa fonction de client DHCP désactivée et doit disposer d'une nouvelle adresse IP statique puisque son adresse IP risque de changer lors de l'utilisation de la fonction DHCP.

- Port Map List (Liste de mappage des ports). Cette section permet de personnaliser le service de port de vos applications.
  - Application. Entrez le nom de l'application dans ce champ.
  - External Port (Port externe) et Internal Port (Port interne). Entrez ensuite les numéros de ports internes et externes.
  - Protocol (Protocole). Sélectionnez le protocole que vous souhaitez utiliser pour chaque application. **TCP** ou **UDP**.
  - IP Address (Adresse IP). Entrez l'adresse IP de l'ordinateur concerné.
  - Enabled (Activé). Cliquez sur **Enabled** (Activé) pour activer le transfert vers l'application choisie.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

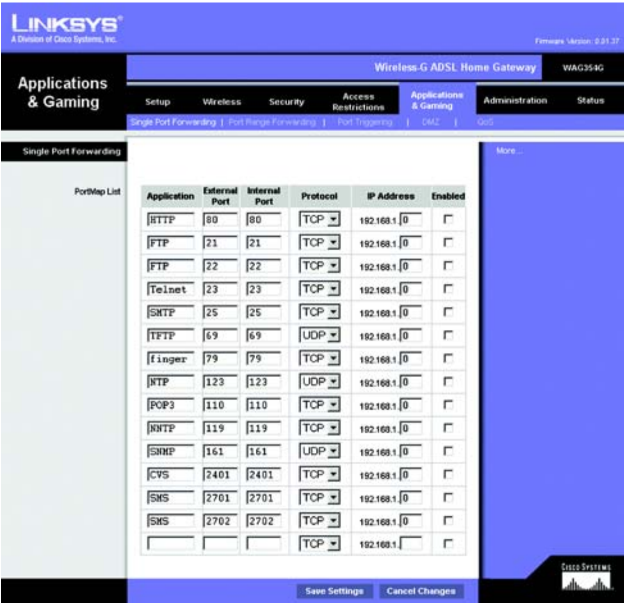


Figure 5-27 : Single Port Forwarding (Transfert de connexion unique)

Onglet Port Range Forwarding (Transfert de connexion)

L'écran *Port Range Forwarding* (Transfert de connexion) définit les services publics de votre réseau, tels que serveurs Web, serveurs FTP, serveurs de messagerie électronique ou toute autre application Internet spécialisée. Par applications spécialisées, on entend toutes les applications qui utilisent un accès Internet pour effectuer des fonctions spécifiques, telles que la vidéoconférence ou les jeux en ligne. Certaines applications Internet peuvent n'exiger aucun transfert.

Lorsque des utilisateurs envoient ce type de requête vers votre réseau via Internet, le modem routeur transfère ces requêtes vers l'ordinateur approprié. Tout ordinateur dont le port est transféré doit avoir sa fonction de client DHCP désactivée et doit disposer d'une nouvelle adresse IP statique puisque son adresse IP risque de changer lors de l'utilisation de la fonction DHCP.

- Application. Entrez le nom de l'application dans ce champ.
- Start (Début) et End (Fin). Entrez les numéros de début et de fin du port que vous souhaitez transférer.
- Protocol (Protocole). Sélectionnez le protocole que vous souhaitez utiliser pour chaque application. **TCP**, **UDP** ou **Both** (Les deux).
- IP Address (Adresse IP). Entrez l'adresse IP de l'ordinateur concerné.
- Enable (Activer). Cochez la case **Enable** (Activer) pour activer le transfert vers l'application choisie.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

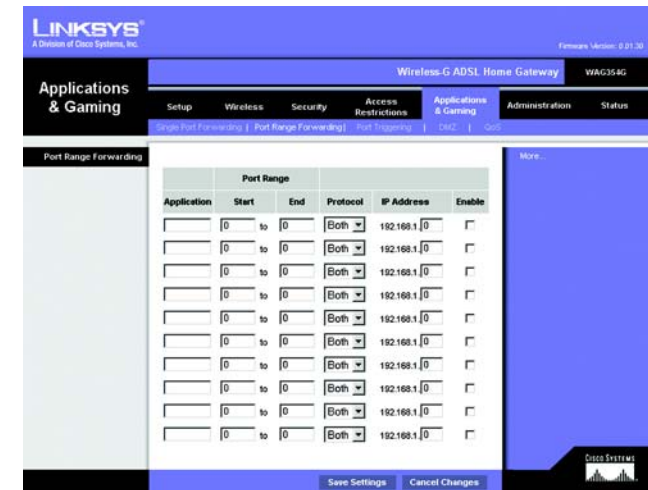


Figure 5-28 : Port Range Forwarding (Transfert de connexion)

Onglet Port Triggering (Déclenchement de connexion)

Le déclenchement de connexion est utilisé pour des applications spécifiques qui peuvent nécessiter l'ouverture d'un port à la demande. Pour cette fonction, le modem routeur contrôle les données sortantes de certains numéros de ports spécifiques. Le modem routeur enregistre l'adresse IP de l'ordinateur qui envoie une requête de données. Ainsi lorsque les données transitent de nouveau par le modem routeur, elles sont dirigées vers l'ordinateur approprié au moyen de l'adresse IP et des règles de mappage de ports.

- Application. Entrez le nom que vous souhaitez donner à chaque application.
- Triggered Range (Connexion sortante déclenchée). Entrez les numéros de port de départ et de fin de la connexion sortante transférée.
- Forwarded Range (Connexion entrante transférée). Entrez les numéros de port de départ et de fin de la connexion entrante transférée.
- Enable (Activer). Cochez la case **Enable** (Activer) pour activer le déclenchement de l'application choisie.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

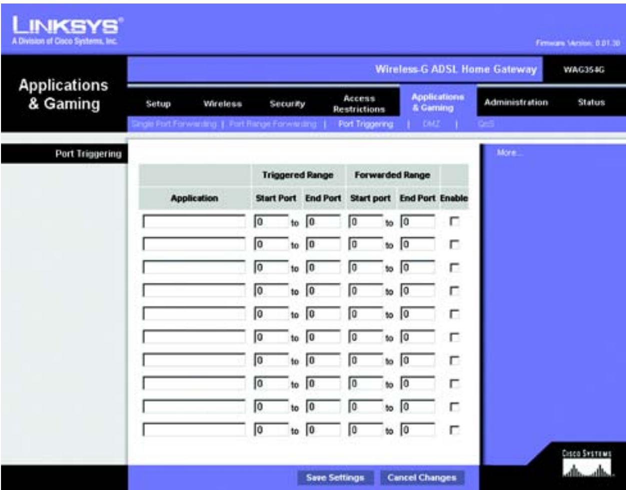


Figure 5-29 : Port Triggering (Déclenchement de connexion)

Onglet DMZ

L'écran *DMZ* permet à un utilisateur local d'accéder à Internet en vue d'utiliser un service à usage spécifique, tel que des jeux Internet ou un système de vidéoconférence via l'hébergement DMZ. L'hébergement DMZ transfère simultanément tous les ports d'un ordinateur, à la différence de l'option Port Range Forwarding (Transfert de connexion) qui ne permet de transférer que 10 connexions au maximum.

- Hébergement DMZ. Cette fonctionnalité permet à un utilisateur local d'accéder à Internet en vue d'utiliser un service à usage spécifique, tel que des jeux Internet ou un système de vidéoconférence. Pour activer cette fonctionnalité, sélectionnez **Enable** (Activer). Pour la désactiver, sélectionnez **Disable** (Désactiver).

- DMZ Host IP Address (Adresse IP de l'hôte DMZ). Pour exposer un ordinateur, entrez l'adresse IP de cet ordinateur. Pour obtenir l'adresse IP d'un ordinateur, reportez-vous à l'« annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet ».

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.



Figure 5-30 : DMZ

Onglet QoS (QS)

QS

La qualité de service (QS) assure un meilleur service aux types de priorité élevée du trafic réseau, pouvant impliquer des applications importantes en temps réel, comme les appels téléphoniques ou la vidéoconférence via Internet.

Enabled/Disabled (Activé/Désactivé). Pour utiliser QS, sélectionnez **Enable** (Activer). Sinon, conservez la valeur par défaut, **Disable** (Désactiver).

QS basée sur une application

La qualité de service basée sur une application gère les informations telles qu'elles sont transmises et reçues. Selon le paramètre de l'écran *QoS* (QS) cette fonction affecte une priorité faible ou élevée aux cinq applications prédéfinies et aux trois applications supplémentaires que vous spécifiez.

High priority (Priorité élevée)/**Medium priority** (Priorité moyenne)/**Low priority** (Faible priorité). Pour chaque application, sélectionnez **High priority** (Priorité élevée) (le trafic de cette file d'attente partage 60 % de la bande passante totale), **Medium priority** (Priorité moyenne) (le trafic de cette file d'attente partage 18 % de la bande passante totale) ou **Low priority** (Priorité faible) (le trafic de cette file d'attente partage 1 % de la bande passante totale).

FTP (File Transfer Protocol). Protocole utilisé pour la transmission de fichiers sur un réseau TCP/IP (Internet, UNIX, etc.). Par exemple, lorsque des pages HTML sont développées pour un site Web sur une machine locale, elles sont généralement téléchargées sur le serveur Web via FTP.

HTTP (HyperText Transport Protocol). Protocole de communication utilisé pour la connexion à des serveurs sur le World Wide Web. Sa principale fonction est d'établir une connexion à un serveur Web et de transmettre les pages HTML au navigateur Web du client.

Telnet. Protocole d'émulation de terminal couramment utilisé sur les réseaux Internet et TCP/IP. Il permet à un utilisateur d'un terminal ou d'un ordinateur de se connecter à un périphérique distant et d'exécuter un programme.

SMTP (Simple Mail Transfer Protocol). Protocole de messagerie standard utilisé sur Internet. Il s'agit d'un protocole TCP/IP qui définit le message et l'agent de transfert de messages (MTA), qui enregistre et transmet les messages.

POP3 (Post Office Protocol 3). Serveur de messagerie standard couramment utilisé sur Internet. Il fournit un emplacement de stockage des messages qui contient les messages entrants jusqu'à ce que les utilisateurs se connectent et les téléchargent. POP3 est un système simple requérant peu de sélections. Tous les messages et pièces jointes en attente sont téléchargés en même temps. POP3 utilise le protocole de messagerie SMTP.

Specific Port# (Numéro de port spécifique). Vous pouvez ajouter trois applications supplémentaires en entrant leur numéro de port respectif dans ces champs.

Lorsque vous avez terminé d'apporter des modifications dans cet écran, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer les modifications ou le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

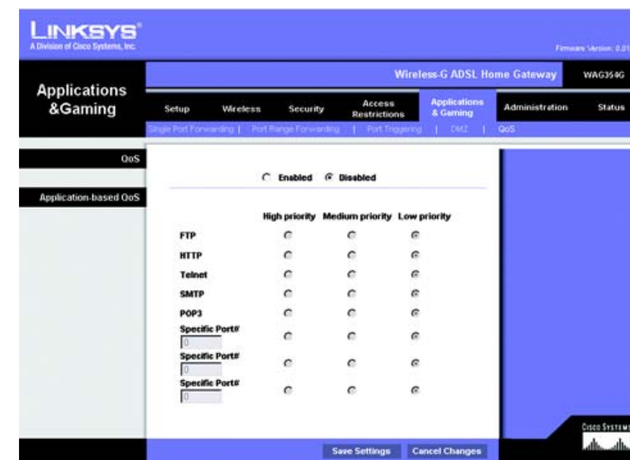


Figure 5-31 : QS

Onglet Administration

Onglet Management (Gestion)

L'écran *Management* (Gestion) vous permet de modifier les paramètres d'accès au modem routeur et de configurer les fonctionnalités de gestion SNMP (Simple Network Management Protocol), UPnP (Universal Plug and Play), proxy IGMP (Internet Group Multicast Protocol) et WLAN.

Gateway Access (Accès au modem routeur)

Local Gateway Access (Accès local au modem routeur). Pour assurer la sécurité du modem routeur, vous devez entrer un mot de passe pour accéder à l'utilitaire Web du modem routeur. Le nom d'utilisateur et le mot de passe par défaut est **admin**.

- Gateway Userlist (Liste d'utilisateurs du modem routeur). Sélectionnez le numéro de l'utilisateur dans le menu déroulant.
- Gateway Username (Nom d'utilisateur du modem routeur). Entrez le nom d'utilisateur par défaut, **admin**. Il est recommandé de remplacer ce nom d'utilisateur par défaut par un nom de votre choix.
- Gateway Password (Mot de passe du modem routeur). Il est recommandé de remplacer le mot de passe par défaut, **admin**, par un mot de passe de votre choix.
- Re-enter to confirm (Confirmation du mot de passe). Entrez de nouveau le nouveau mot de passe du modem routeur pour le confirmer.

Remote Gateway Access (Accès distant au modem routeur). Cette fonction vous permet d'accéder au modem routeur à partir d'un emplacement distant, via Internet.

- Gestion distante. Cette fonction vous permet d'administrer le modem routeur à partir d'un emplacement distant, via Internet. Pour activer la gestion à distance, cliquez sur **Enable** (Activer).



IMPORTANT : L'activation de la gestion distante permet à chaque personne disposant de votre mot de passe de configurer à distance le modem routeur via Internet.

- Port de gestion. Entrez le numéro de port que vous souhaitez utiliser pour accéder à distance au modem routeur.
- IP autorisé. Spécifiez la ou les adresses IP autorisées à gérer le modem routeur à distance. Pour autoriser toutes les adresses IP sans restriction, sélectionnez **All** (Toutes). Pour spécifier une seule adresse IP, sélectionnez

Figure 5-32 : Management (Gestion)

Figure 5-33 : IP autorisé - Plage IP

IP address (Adresse IP) et entrez l'adresse dans les champs réservés à cet effet. Pour spécifier une plage d'adresses IP, sélectionnez **IP range** (Plage IP) et entrez la plage d'adresses dans les champs réservés à cet effet.

Mise à jour à distance. Cette fonction permet une mise à jour à distance du micrologiciel du modem routeur avec un serveur TFTP. Pour activer la mise à jour à distance, cliquez sur **Enable** (Activer).

SNMP

SNMP est un protocole très répandu de contrôle et de gestion réseau. Pour activer le SNMP, cliquez sur **Activé.** Pour désactiver le SNMP, cliquez sur **Désactivé.**

S'il est désactivé, spécifiez la ou les adresses IP ayant un accès SNMP. Sélectionnez **All** (Toutes) pour autoriser toutes les adresses sans restriction, **IP address** (Adresse IP) pour spécifier une seule adresse ou **IP range** (Plage IP) pour spécifier une plage d'adresses.

- Device Name (Nom de périphérique) : Entrez le nom du modem routeur.
- SNMP v1/v2 : Get Community (Obtenir la communauté). Entrez le mot de passe permettant l'accès en lecture seule aux informations SNMP du modem routeur.
- Set Community (Définir la communauté). Entrez le mot de passe permettant l'accès en lecture/écriture aux informations SNMP du modem routeur.
- Gestion du déroutement : Dérouter vers. Entrez l'adresse IP de l'ordinateur hôte distant auquel s'adressent les messages déroutés.

UPnP

La fonctionnalité UPnP permet à Windows Me et XP de configurer automatiquement le modem routeur pour diverses applications Internet, telles que des jeux Internet ou un système de vidéoconférence.

- UPnP : Pour activer la fonctionnalité UPnP, cliquez sur **Enable** (Activée). Sinon, cliquez sur **Disable** (Désactivée).

Proxy IGMP

Si votre périphérique ou votre application multimédia ne fonctionnent pas correctement derrière le modem routeur, vous pouvez activer le proxy IGMP pour autoriser la multidiffusion via le modem routeur.

- Proxy IGMP. Pour activer cette fonctionnalité, sélectionnez **Enable** (Activer). Pour désactiver le son, sélectionnez **Disable** (Désactiver).

WLAN

- Gestion via WLAN. Cette fonction vous permet d'administrer le modem routeur sur un ordinateur sans fil du réseau local lorsqu'il est connecté à l'utilitaire Web du modem routeur.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Onglet Reporting (Rapports)

L'écran *Reporting* (Rapports) fournit un fichier journal de toutes les URL ou adresses IP entrantes et sortantes de votre connexion Internet. Il fournit également des fichiers journaux de tous les événements VPN et de pare-feu.

Reporting (Rapports)

- Log (Fichier journal). Pour activer la génération de fichiers journaux, cliquez sur **Enabled** (Activée).
- Logviewer IP Address (Adresse IP de réception des fichiers journaux). Entrez l'adresse IP de l'ordinateur qui doit recevoir les journaux. Pour afficher ces journaux, vous devez utiliser le logiciel Logviewer. Vous pouvez télécharger ce logiciel gratuit depuis le site www.linksys.com.

Email Alerts (Alertes de messagerie électronique)

- E-Mail Alerts (Alertes de messagerie électronique). Pour activer les alertes de messagerie électronique, cliquez sur **Enabled** (Activées).
- Denial of Service Thresholds (Seuils de refus de service). Entrez le nombre d'attaques DoS (Denial of Service) qui déclencheront une alerte par courrier électronique.
- SMTP Mail Server (Serveur de messagerie électronique SMTP). Entrez l'adresse IP du serveur SMTP.
- E-Mail Address for Alert Logs (Adresse de messagerie électronique pour fichiers journaux d'alertes). Entrez l'adresse électronique pour la réception des journaux d'alertes.
- Return E-Mail address (Adresse de messagerie électronique de retour). Entrez l'adresse de retour des alertes de messagerie électronique.

Pour afficher les fichiers journaux, cliquez sur le bouton **View Logs** (Afficher les fichiers journaux). Un nouvel écran apparaît. Dans le menu déroulant, sélectionnez le journal que vous souhaitez afficher. Cliquez sur le bouton **Clear** (Supprimer) pour supprimer les informations. Cliquez sur le bouton **pageRefresh** (Actualiser la page) pour



Figure 5-34 : Reporting (Rapports)



Figure 5-35 : Fichier journal système

mettre à jour les informations. Cliquez sur le bouton **Previous Page** (Page précédente) pour revenir à la page précédente. Cliquez sur le bouton **Next Page** (Page suivante) pour accéder à la page suivante.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Onglet Diagnostics

Ping Test (Test Ping)

Ping Test Parameters (Paramètres de test Ping)

- Ping Target IP (IP de cible Ping). Entrez l'adresse IP pour laquelle vous souhaitez effectuer le test Ping. Il peut s'agir d'une adresse IP locale (LAN) ou Internet (WAN).
- Ping Size (Taille de Ping). Entrez la taille du paquet.
- Number of Pings (Nombre de Pings). Entrez le nombre de fois que vous souhaitez effectuer le Ping.
- Ping Interval (Intervalle de Ping). Entrez l'intervalle de Ping (fréquence du Ping de l'adresse IP cible) en millisecondes.
- Ping Timeout (Délai de Ping). Entrez le délai de Ping (délai avant la fin du Ping) en millisecondes.

Cliquez sur le bouton **Start Test** (Démarrer le test) pour démarrer le test de Ping.

- Ping Result (Résultat de Ping). Les résultats du test Ping sont affichés ici.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Onglet Backup&Restore (Sauvegarde&restauration)

Cet onglet permet de sauvegarder et de restaurer le fichier de configuration du modem routeur.

Sauvegarder la configuration

Pour sauvegarder le fichier de configuration du modem routeur, cliquez sur le bouton **Backup** (Sauvegarder). Suivez les instructions affichées.



Figure 5-36 : Ping Test (Test Ping)



Figure 5-37 : Backup&Restore (Sauvegarde et restauration)

Restaurer la configuration

Pour restaurer le fichier de configuration du modem routeur, cliquez sur le bouton **Browse** (Parcourir). Puis suivez les instructions affichées pour localiser le fichier. Après avoir sélectionné le fichier, cliquez sur le bouton **Restore** (Restaurer).

Onglet Factory Defaults (Paramètres usine par défaut)

Restore Factory Defaults (Restaurer les paramètres d'usine) : Si vous souhaitez restaurer les paramètres d'usine du modem routeur (vous perdrez alors tous vos paramètres), cliquez sur **Yes** (Oui).

Pour débuter le processus de restauration, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer ces modifications ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour annuler les modifications effectuées.



Figure 5-38 : Factory Defaults (Paramètres usine par défaut)

Onglet Firmware Upgrade (Mise à jour du micrologiciel)

Le modem routeur permet de mettre à niveau le micrologiciel côté LAN (réseau) du modem routeur.

Upgrade from LAN (Mise à jour à partir du réseau LAN)

Pour mettre à niveau le micrologiciel du modem routeur à partir du réseau LAN :

1. Téléchargez le fichier de mise à jour du micrologiciel du modem routeur depuis le site www.linksys.com/fr.
2. Extrayez le fichier sur votre ordinateur.
3. Cliquez sur le bouton **Browse** (Parcourir) pour rechercher le fichier de mise à jour du micrologiciel.
4. Cliquez deux fois sur le fichier du micrologiciel que vous venez de télécharger et de décompresser.
5. Cliquez sur le bouton **Upgrade** (Mise à jour) et suivez les instructions affichées.

Pour annuler la mise à jour du micrologiciel, cliquez sur le bouton **Cancel Upgrade** (Annuler mise à jour).



Figure 5-39 : Firmware Upgrade (Mise à jour du micrologiciel)

Onglet Reboot (Redémarrage)

Cet écran permet d'effectuer un redémarrage logiciel ou matériel du modem routeur. En général, vous utiliserez le redémarrage matériel. Le redémarrage logiciel est identique à l'opération qui consiste à redémarrer l'ordinateur, sans toutefois mettre physiquement l'ordinateur hors tension.

Reboot (Redémarrage)

Mode de redémarrage. Pour redémarrer le modem routeur, sélectionnez **Hard** (Matériel) ou **Soft** (Logiciel). Sélectionnez **Hard** (Matériel) pour lancer le cycle d'alimentation du modem routeur ou **Soft** (Logiciel) pour le redémarrer sans recourir au cycle d'alimentation.

Pour lancer la procédure de redémarrage, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres). Lorsqu'un écran s'affiche pour vous demander si vous souhaitez redémarrer le modem routeur, cliquez sur **OK.**

Cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour annuler le redémarrage.



Figure 5-40 : Reboot (Redémarrage)

Onglet Status (Etat)

Onglet Gateway (Modem routeur)

Cet écran contient des informations sur votre modem routeur et sa connexion Internet.

Gateway Information (Informations sur le modem routeur)

Cette section contient les éléments suivants : Firmware Version (Version du micrologiciel) du modem routeur, MAC Address (Adresse Mac) et Current Time (Heure actuelle).

Connexion Internet

Cette section contient les éléments suivants : Connection (Connexion), Login Type (Type de connexion), Interface, IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau), Default Gateway (Passerelle par défaut), adresses IP des serveurs DNS 1, 2 et 3 et adresse WINS.

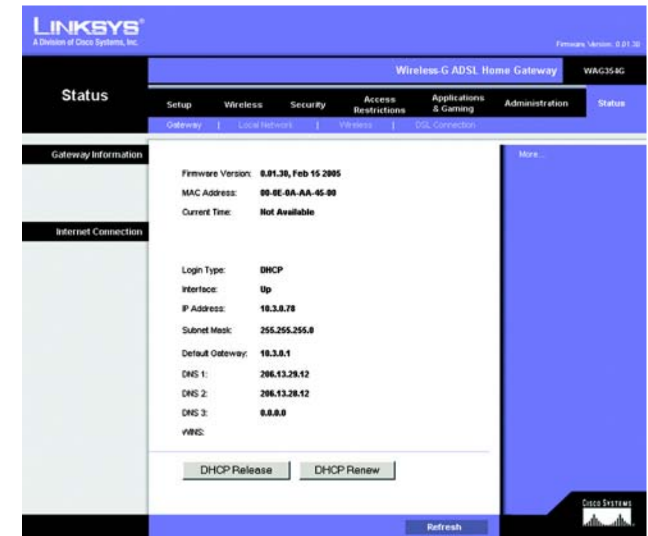


Figure 5-41 : Gateway (Modem routeur)

DHCP Renew (Renouvellement DHCP). Cliquez sur le bouton **DHCP Renew** (Renouvellement DHCP) pour remplacer l'adresse IP actuelle du modem routeur par une nouvelle adresse IP.

DHCP Release (Version DHCP). Cliquez sur le bouton **DHCP Release** (Version DHCP) pour supprimer l'adresse IP actuelle du modem routeur.

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées.

Onglet Local Network (Réseau local)

Cette section contient les éléments suivants : local Mac Address (Adresse Mac locale), IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau), DHCP Server (Serveur DHCP), Start IP Address (Adresse IP de début) et End IP Address (Adresse IP de fin). Pour afficher le tableau des clients DHCP, cliquez sur le bouton **DHCP Clients Table** (Tableau des clients DHCP). Pour afficher le tableau ARP/RARP, cliquez sur le bouton **ARP/RARP Table** (Tableau ARP/RARP).

DHCP Clients Table (Tableau des clients DHCP). Le tableau des clients DHCP affiche les données actuelles des clients DHCP. Vous verrez les informations suivantes : nom de l'ordinateur, adresse IP, adresse MAC et délai d'expiration de l'adresse IP dynamique des clients sans fil utilisant le serveur DHCP. Les données sont stockées dans la mémoire temporaire et sont régulièrement modifiées. Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Pour supprimer un client d'un serveur DHCP, sélectionnez le client, puis cliquez sur le bouton **Delete** (Supprimer). Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran *Local Network* (Réseau local).

Tableau ARP/RARP. Le tableau ARP/RARP affiche les données actuelles des clients du réseau local ayant envoyé une requête ARP au modem routeur. Vous verrez apparaître leurs adresses IP et MAC. Les données sont stockées dans la mémoire temporaire et sont régulièrement modifiées. Une requête ARP est une requête envoyée du modem routeur aux clients ayant une adresse IP pour leur demander leurs adresses MAC. Le modem routeur peut ainsi établir une correspondance entre les adresses IP et les adresses MAC. RARP est le contraire de ARP. Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran *Local Network* (Réseau local).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées.



Figure 5-42 : Local Network (Réseau local)

DHCP Active IP Table

DHCP Server IP Address: **192.168.1.1**

Client Host Name	IP Address	MAC Address	Expires
None	None	None	None

Refresh · Delete · Close

Figure 5-43 : Table IP active DHCP

ARP/RARP Table

IP Address	MAC Address
192.168.1.64	00:D0:B7:B6:46:BA

Close · Refresh

Figure 5-44 : Tableau ARP/RARP

Onglet Wireless (Sans fil)

Cette section contient les éléments suivants : Wireless Firmware Version (Version du micrologiciel), MAC Address (Adresse MAC), Mode, SSID, DHCP Server (Serveur DCP), Channel (Canal) et Encryption Function (Fonction de cryptage).

Cliquez sur le bouton **Wireless Clients Connected** (Clients sans fil connectés) pour afficher les clients sans fil connectés au modem routeur, ainsi que leurs noms d'ordinateurs, adresses IP et adresses Mac. Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées. Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran *Wireless* (Sans fil).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées.



Figure 5-45 : Wireless (Sans fil)



Figure 5-46 : Ordinateurs réseau

Onglet DSL Connection (Connexion DSL)

Cet écran contient des informations sur les connexions DSL et PVC.

Etat DSL

Cette section contient les éléments suivants : DSL Status (Etat DSL), DSL Modulation Mode (Mode de modulation DSL), DSL Path Mode (Mode du chemin DSL), Downstream Rate (Débit de réception), Upstream Rate (Débit d'émission), Downstream Margin (Marge de réception), Upstream Margin (Marge d'émission), Downstream Line Attenuation (Affaiblissement de la ligne de réception), Upstream Line Attenuation (Affaiblissement de la ligne d'émission), Downstream Transmit Power (Puissance à la réception) et Upstream Transmit Power (Puissance à l'émission).

Connexion PVC

Cette section contient les éléments suivants : Encapsulation, Multiplexing (Multiplexage), QoS (QS), Pcr Rate (Taux Pcr), Scr Rate (Taux Scr), Autodetect (Détection automatique), VPI, VCI et PVC Status (Etat PVC).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser les informations affichées.

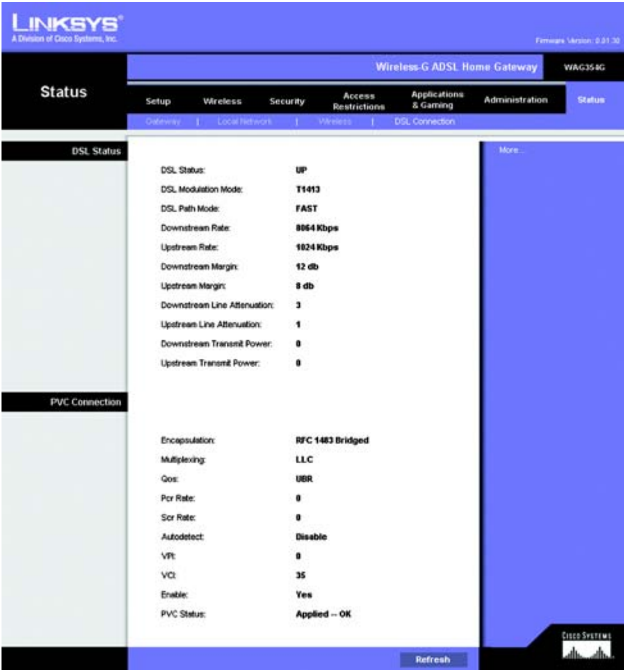


Figure 5-47 : DSL Connection (Connexion DSL)

Annexe A : Dépannage

Cette annexe comporte deux parties : « Problèmes courants et solutions » et « Questions fréquemment posées ». Elle contient des solutions envisageables aux problèmes susceptibles de se produire lors de l'installation et de l'exploitation du modem routeur. Lisez les descriptions ci-dessous pour vous aider à résoudre vos problèmes. Si vous n'y trouvez aucune réponse, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

Problèmes courants et solutions

1. Je souhaite définir une adresse IP statique sur un ordinateur.

Vous pouvez attribuer une adresse IP statique à un ordinateur en procédant comme suit :

- Windows 98 et Windows Me :
    1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois sur **Réseau**.
    2. Dans la zone Les composants réseau suivants sont installés, sélectionnez le composant TCP/IP associé à votre adaptateur Ethernet. Si un seul adaptateur Ethernet est installé, une seule ligne TCP/IP apparaît sans association à un adaptateur Ethernet. Mettez-la en surbrillance, puis cliquez sur le bouton Propriétés.
    3. Dans la fenêtre Propriétés TCP/IP, sélectionnez l'onglet Adresse IP, puis l'option Spécifier une adresse IP. Entrez une adresse IP unique utilisée par aucun autre ordinateur du réseau connecté au modem routeur. Assurez-vous que chaque adresse IP est unique pour chaque ordinateur ou périphérique du réseau.
    4. Cliquez sur l'onglet **Passerelle**, puis tapez 192.168.1.1 dans le champ Nouvelle passerelle, c'est-à-dire l'adresse IP de passerelle par défaut. Cliquez sur le bouton Ajouter pour valider cette entrée.
    5. Cliquez sur l'onglet **Configuration DNS** et assurez-vous que l'option Désactiver DNS est sélectionnée. Entrez les noms de l'hôte et du domaine (par exemple, Jean pour l'hôte et « domicile » pour le domaine). Entrez le DNS fourni par votre fournisseur d'accès Internet (FAI). Si votre FAI ne vous a fourni aucune adresse IP DNS, contactez-le pour obtenir cette information ou recherchez l'information en question sur son site Web.
    6. Cliquez sur le bouton **OK** dans la fenêtre Propriétés TCP/IP, puis cliquez sur Fermer ou sur OK dans la fenêtre Réseau.
    7. Redémarrez l'ordinateur dès que le système vous le demande.
- Sous Windows 2000 :
    1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois sur **Connexions réseau et accès à distance**.
    2. Cliquez à l'aide du bouton droit de la souris sur la Connexion au réseau local associée à l'adaptateur Ethernet que vous utilisez, puis sélectionnez l'option Propriétés.

3. Dans la zone Les composants sélectionnés sont utilisés par cette connexion, mettez l'option **Protocole Internet (TCP/IP)** en surbrillance, puis sélectionnez l'option Propriétés. Sélectionnez l'option **Utiliser l'adresse IP suivante.**
4. Entrez une adresse IP unique utilisée par aucun autre ordinateur du réseau connecté au modem routeur.
5. Entrez le masque de sous-réseau 255.255.255.0.
6. Entrez l'adresse IP de passerelle par défaut : 192.168.1.1.
7. Dans la partie inférieure de la fenêtre, sélectionnez l'option Utiliser l'adresse de serveur DNS suivante, puis entrez le serveur DNS préféré et le serveur DNS auxiliaire (fournis par votre FAI). Contactez votre FAI ou consultez son site Web pour vous procurer cette information.
8. Cliquez sur **OK** dans la fenêtre Propriétés de Protocole Internet (TCP/IP), puis de nouveau sur **OK** dans la fenêtre Propriétés de Connexion au réseau local.
9. Redémarrez l'ordinateur si le système vous le demande.

- Sous Windows XP :

  Les instructions ci-après supposent que vous utilisez l'interface par défaut de Windows XP. Si vous utilisez l'interface Classique (où les icônes et les menus se présentent comme dans les versions précédentes de Windows), suivez les instructions fournies pour Windows 2000.

  1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration.**
  2. Cliquez sur l'icône **Connexions réseau et Internet**, puis sur l'icône **Connexions réseau.**
  3. Cliquez à l'aide du bouton droit de la souris sur la **Connexion au réseau local** associée à l'adaptateur Ethernet que vous utilisez, puis sélectionnez l'option Propriétés.
  4. Dans la zone **Cette connexion utilise les éléments suivants**, mettez l'option **Protocole Internet (TCP/IP)** en surbrillance. Cliquez sur le bouton **Propriétés.**
  5. Entrez une adresse IP unique utilisée par aucun autre ordinateur du réseau connecté au modem routeur.
  6. Entrez le masque de sous-réseau 255.255.255.0.
  7. Entrez l'adresse IP de passerelle par défaut: 192.168.1.1.
  8. Dans la partie inférieure de la fenêtre, sélectionnez l'option Utiliser l'adresse de serveur DNS suivante, puis entrez le serveur DNS préféré et le serveur DNS auxiliaire (fournis par votre FAI). Contactez votre FAI ou consultez son site Web pour vous procurer cette information.
  9. Cliquez sur le bouton **OK** dans la fenêtre Propriétés de Protocole Internet (TCP/IP). Cliquez sur le bouton **OK** dans la fenêtre Propriétés de Connexion au réseau local.

2. Je souhaite tester ma connexion Internet.

A. Vérifiez vos paramètres TCP/IP.

Windows 98, Me, 2000 et XP :

- Pour plus de détails, reportez-vous à l'aide de Windows. Assurez-vous que l'option Obtenir une adresse IP automatiquement est sélectionnée dans les paramètres.

Windows NT 4.0 :

- Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois sur l'icône **Réseau.**

- Cliquez sur l'onglet Protocole, puis double-cliquez sur le protocole TCP/IP.
- Dans la fenêtre qui s'affiche, assurez-vous que vous avez sélectionné l'adaptateur approprié et définissez-le à **Obtenir une adresse IP à partir d'un serveur DHCP**.
- Cliquez sur le bouton **OK** dans la fenêtre Propriétés TCP/IP, puis cliquez sur le bouton **Fermer** dans la fenêtre Réseau.
- Redémarrez l'ordinateur si le système vous le demande.

B. Ouvrez une invite de commande.

Windows 98 et Windows Me :

- Cliquez sur **Démarrer**, puis sélectionnez **Exécuter.** Dans le champ Ouvrir, tapez command. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK.**

Windows NT, 2000 et XP :

- Cliquez sur **Démarrer**, puis sélectionnez **Exécuter.** Dans le champ Ouvrir, tapez cmd. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK.** Dans l'invite de commande, tapez ping 192.168.1.1, puis appuyez sur la touche Entrée.
- Si vous obtenez une réponse, cela signifie que l'ordinateur communique avec le modem routeur.
- Si vous n'obtenez PAS de réponse, vérifiez le câble et assurez-vous que l'option Obtenir une adresse IP automatiquement est sélectionnée dans les paramètres TCP/IP de votre adaptateur Ethernet.

C. Dans l'invite de commande, tapez la commande ping suivie de votre adresse IP Internet ou WAN, puis appuyez sur la touche **Entrée.** Vous pouvez vous procurer l'adresse IP Internet ou WAN dans l'écran Etat de l'utilitaire Web du modem routeur. Par exemple, si votre adresse IP Internet ou WAN est 1.2.3.4, vous devez entrer la commande ping 1.2.3.4, puis appuyer sur la touche Entrée.

- Si vous obtenez une réponse, cela signifie que l'ordinateur est connecté au modem routeurau modem routeur.
- Si vous n'obtenez PAS de réponse, essayez d'appliquer la commande Ping à partir d'un autre ordinateur pour vérifier s'il s'agit de l'ordinateur d'origine qui est la cause du problème.

D. Dans l'invite de commande, tapez ping www.yahoo.com, puis appuyez sur la touche **Entrée.**

- Si vous obtenez une réponse, c'est le signe que l'ordinateur est connecté à Internet. Si vous ne parvenez pas à ouvrir une page Web, exécutez la commande Ping à partir d'un autre ordinateur pour vérifier s'il s'agit de l'ordinateur d'origine qui est la cause du problème.
- Si vous n'obtenez PAS de réponse, le problème est peut-être lié à la connexion. Essayez d'appliquer la commande Ping à partir d'un autre ordinateur pour vérifier s'il s'agit de l'ordinateur d'origine qui est la cause du problème.

3. *Je n'obtiens aucune adresse IP sur Internet par le biais de ma connexion Internet.*

- Reportez-vous au problème 2 (Je souhaite tester ma connexion Internet) pour vérifier votre connectivité.
  1. Assurez-vous que vous utilisez les paramètres de connexion Internet corrects. Contactez votre FAI pour savoir si votre connexion Internet est de type RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE ou RFC 2364 PPPoA. Reportez-vous à la section Configuration du « Chapitre 5 : Configuration

du modem routeur ADSL résidentiel sans fil G » pour obtenir des informations détaillées sur les paramètres de connexion Internet.

2. Assurez-vous que vous disposez du câble approprié. Vérifiez si le voyant ADSL du modem routeur est allumé.
3. Assurez-vous que le câble reliant le port ADSL du modem routeur est connecté à la prise murale ADSL. Vérifiez que la page Status (Etat) de l'utilitaire Web du modem routeur indique une adresse IP valide fournie par votre FAI.
4. Eteignez l'ordinateur et le modem routeur. Attendez 30 secondes puis allumez de nouveau le modem routeur et l'ordinateur. Vérifiez que vous disposez bien d'une adresse IP dans l'onglet Status (Etat) de l'utilitaire Web du modem routeur.

4. Je ne parviens pas à accéder à la page de configuration de l'utilitaire Web du modem routeur.

- Reportez-vous au « Problème 2 : Je souhaite tester ma connexion Internet » pour vérifier que votre ordinateur est correctement connecté au modem routeur.
  1. Reportez-vous à l'« annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet » pour vérifier que votre ordinateur possède bien une adresse IP, un masque de sous-réseau, une passerelle et une adresse DNS.
  2. Définissez une adresse IP statique sur votre système. Reportez-vous au « Problème 1 : Je dois définir une adresse IP statique ».
  3. Reportez-vous au « Problème 10 : Je dois supprimer les paramètres de proxy ou la fenêtre de connexion à distance (pour les utilisateurs PPPoE) ».

5. Mon VPN (Virtual Private Network) ne fonctionne pas via le modem routeur.

Accédez à l'interface Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur, puis sélectionnez l'onglet Security (Sécurité). Assurez-vous que l'intercommunication IPsec et/ou l'intercommunication PPTP sont activés.

- Les VPN qui utilisent l'authentification IPSec avec ESP (Encapsulation Security Payload, qui porte également le nom de Protocole 50) fonctionnent alors correctement. Au moins une session IPSec fonctionne via le modem routeur. Néanmoins, il est possible d'ouvrir plusieurs sessions IPSec simultanément, en fonction des spécifications de vos VPN.
- Les VPN qui utilisent IPSec et AH (Authentication Header, qui porte également le nom de Protocole 51) sont incompatibles avec le modem routeur. AH est soumis à des limitations en raison d'une incompatibilité occasionnelle avec la norme NAT.
- Remplacez l'adresse IP du modem routeur par un autre sous-réseau, afin d'éviter les conflits entre l'adresse IP du VPN et votre adresse IP locale. Par exemple, si votre serveur VPN attribue une adresse IP 192.168.1.X (X étant un numéro entre 1 et 254) et que votre adresse IP LAN locale est 192.168.1.X (X étant le même numéro utilisé dans l'adresse IP VPN), le modem routeur aura des difficultés à envoyer les informations vers l'emplacement correct. Si vous changez l'adresse IP du modem routeur en 192.168.2.1, le problème devrait être résolu. Changez l'adresse IP du modem routeur dans l'onglet Setup (Configuration) de l'interface Web.

- Si vous avez attribué une adresse IP statique à un ordinateur ou périphérique du réseau, vous devez changer son adresse IP en 192.168.2.Y (Y étant n'importe quel nombre entre 1 et 254). Veuillez noter que chaque adresse IP doit être unique sur le réseau.
- Votre VPN peut exiger l'envoi de paquets port 500/UDP vers l'ordinateur connecté au serveur IPSec. Pour plus d'informations, reportez-vous au « Problème 7 : Je souhaite configurer un hébergement pour jeux en ligne ou utiliser d'autres applications Internet. »
- Pour plus d'informations, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

6. *Je souhaite configurer un serveur derrière ma modem routeur et le rendre accessible au public.*

Pour utiliser un serveur tel qu'un serveur de messagerie, un serveur Web ou FTP, vous devez connaître les numéros de port utilisés. Par exemple, le port 80 (HTTP) est utilisé pour le Web, le port 21 (FTP) pour le FTP et les ports 25 (SMTP sortant) et 110 (POP3 entrant) pour le serveur de messagerie. Pour obtenir plus d'informations, reportez-vous à la documentation fournie avec le serveur que vous avez installé.

- Pour configurer le transfert de connexion via l'utilitaire Web du modem routeur, procédez comme suit : Nous allons configurer des serveurs Web, FTP et de messagerie.
  1. Accédez à l'utilitaire Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur. Cliquez sur Applications and Gaming (Applications et jeux), puis sur Port Range Forwarding (Transfert de connexion).
  2. Entrez dans ce champ le nom que vous souhaitez donner à l'application personnalisée.
  3. Entrez l'étendue des ports externes du service que vous utilisez. Par exemple, si vous utilisez un serveur Web, entrez l'étendue 80 à 80.
  4. Vérifiez le protocole que vous allez utiliser : TCP et/ou UDP.
  5. Entrez l'adresse IP de l'ordinateur ou du périphérique réseau auquel vous souhaitez que le serveur de port accède. Par exemple, si l'adresse IP de l'adaptateur Ethernet du serveur Web est 192.168.1.100, entrez 100 dans le champ. Reportez-vous à l'« annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet » pour plus d'informations sur l'obtention d'une adresse IP.
  6. Activez la case à cocher Enable (Activer) correspondant au service des ports à utiliser. Prenons l'exemple suivant :

Application personnalisée	Port externe	TCP	UDP	Adresse IP	Activer
Serveur Web	80 à 80	X		192.168.1.100	X
Serveur FTP	21 à 21	X		192.168.1.101	X
SMTP (sortant)	25 à 25	X		192.168.1.102	X
POP3 (entrant)	110 à 110	X		192.168.1.102	X

Une fois la configuration terminée, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

7. Je dois configurer un hébergement pour jeux en ligne ou utiliser d'autres applications Internet.

Si vous souhaitez jouer en ligne ou utiliser des applications Internet, la plupart des opérations fonctionnent sans aucun transfert de connexion ou hébergement DMZ. Il se peut, dans certains cas, que vous souhaitiez héberger un jeu en ligne ou une application Internet. Vous devez dans ce cas configurer le modem routeur pour qu'elle envoie les paquets entrants ou les données entrantes vers un ordinateur spécifique. Ceci s'applique également aux applications Internet que vous utilisez. Pour connaître les ports à utiliser, le mieux est de consulter directement le site Web des jeux en ligne ou des applications. Pour configurer l'hébergement de jeux en ligne ou utiliser une application Internet spécifique, procédez comme suit :

1. Accédez à l'interface Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur. Cliquez sur Applications and Gaming (Applications et jeux), puis sur Port Range Forwarding (Transfert de connexion).
2. Entrez dans ce champ le nom que vous souhaitez donner à l'application personnalisée.
3. Entrez l'étendue des ports externes du service que vous utilisez. Par exemple, si vous souhaitez héberger Unreal Tournament (UT), entrez l'étendue 7777 à 27900.
4. Vérifiez le protocole que vous allez utiliser : TCP et/ou UDP.
5. Entrez l'adresse IP de l'ordinateur ou du périphérique réseau auquel vous souhaitez que le serveur de port accède. Par exemple, si l'adresse IP de l'adaptateur Ethernet du serveur Web est 192.168.1.100, entrez 100 dans le champ. Reportez-vous à l'« annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet » pour plus d'informations sur l'obtention d'une adresse IP.
6. Activez la case à cocher **Enable** (Activer) correspondant au service des ports à utiliser. Prenons l'exemple suivant :

Application personnalisée	Port externe	TCP	UDP	Adresse IP	Activer
UT	7777 à 27900	X	X	192.168.1.100	X
Halflife	27015 à 27015	X	X	192.168.1.105	X
PC Anywhere	5631 à 5631		X	192.168.1.102	X
VPN IPSEC	500 à 500		X	192.168.1.100	X

Une fois la configuration terminée, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

8. Le jeu Internet, le serveur ou l'application ne fonctionne pas.

Si vous rencontrez des difficultés à faire fonctionner correctement un jeu Internet, un serveur ou une application, exposez un ordinateur à Internet à l'aide de l'hébergement DMZ (DeMilitarized Zone). Cette option peut être utilisée lorsqu'une application requiert trop de ports ou lorsque vous ne connaissez pas les services de ports à utiliser. Assurez-vous que toutes les entrées de transfert sont désactivées si vous souhaitez utiliser l'hébergement DMZ. Le transfert a en effet priorité sur l'hébergement DMZ. En d'autres termes, les données qui accèdent au modem routeur seront d'abord contrôlées par les paramètres de transfert. Si le numéro de port d'accès des données accèdent n'est pas soumis au transfert de connexion, le modem routeur transmet les données à l'ordinateur ou au périphérique réseau défini pour l'hébergement DMZ.

- Pour définir l'hébergement DMZ, procédez comme suit :
  1. Accédez à l'utilitaire Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur. Cliquez sur Applications and Gaming (Applications et jeux), puis sur DMZ. Cliquez sur Enabled (Activé) et entrez l'adresse IP de l'ordinateur.
  2. Contrôlez les pages Port Forwarding (Transfert de connexion) et désactivez les entrées que vous avez spécifiées pour le transfert. Conservez ces informations au cas où vous souhaiteriez les utiliser ultérieurement.
- Une fois la configuration terminée, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

9. ***J'ai oublié mon mot de passe ou l'invite de mot de passe apparaît toujours lorsque j'enregistre des paramètres du modem routeur.***
   - Réinitialisez le modem routeur vers les paramètres d'usine. Pour cela, appuyez sur le bouton Reset (Réinitialisation) pendant 10 secondes puis relâchez-le. Si le système vous demande toujours votre mot de passe lors de l'enregistrement des paramètres, procédez comme suit :
     1. Accédez à l'utilitaire Web du modem routeur en spécifiant http://192.168.1.1 ou l'adresse IP du modem routeur. Entrez le nom d'utilisateur et le mot de passe par défaut **admin** (pour les deux) puis cliquez sur l'onglet **Administrations** (Administrations) => **Management** (Gestion).
     2. Entrez un nouveau mot de passe dans le champ Gateway Password (Mot de passe du modem routeur) et entrez le même mot de passe dans le second champ pour confirmation.
     3. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

10. ***Je dois supprimer les paramètres de proxy ou la fenêtre de connexion à distance (pour les utilisateurs PPPoE).***
    Si vous disposez de paramètres de proxy, vous devez les désactiver sur votre ordinateur. Le modem routeur étant destinée à la connexion Internet, l'ordinateur n'a pas besoin des paramètres de proxy pour l'accès à Internet. Pour vérifier que vos paramètres de proxy sont supprimés et que le navigateur que vous utilisez est défini pour se connecter directement au réseau local (LAN), procédez comme suit :

   - Pour Microsoft Internet Explorer 5.0 ou version ultérieure :
     1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois sur Options Internet.
     2. Cliquez sur l'onglet **Connexions.**
     3. Cliquez sur le bouton **Paramètres réseau** et désactivez toutes les cases à cocher.
     4. Cliquez sur le bouton **OK** pour revenir à l'écran précédent.
     5. Activez la case à cocher **Ne jamais établir de connexion.** Vous supprimez ainsi toutes les invites de connexion à distance pour les utilisateurs PPPoE.

   - Pour Netscape 6 et versions supérieures :
     1. Démarrez **Netscape Navigator** et cliquez sur **Edition**, **Préférences**, **Avancé** et **Proxies.**
     2. Assurez-vous que la connexion directe à Internet est sélectionnée à l'écran.
     3. Fermez toutes les fenêtres pour terminer.

11. Pour recommencer, je dois redéfinir le modem routeur aux réglages d'usine.

Appuyez pendant 10 secondes sur le bouton **Reset** (Réinitialiser), puis relâchez-le. Les paramètres Internet, le mot de passe, le transfert ainsi que tous les autres paramètres sont redéfinis aux réglages d'usine. En d'autres termes, le modem routeur revient à sa configuration initiale.

12. Je dois mettre le micrologiciel à niveau.

Pour mettre à niveau le micrologiciel avec les dernières fonctionnalités, vous devez accéder au site Web international de Linksys (www.linksys.com/international) et télécharger la dernière version du micrologiciel.

- Procédez comme suit :
  1. Accédez au site Web international de Linksys à www.linksys.com/international et sélectionnez votre région ou pays.
  2. Cliquez sur l'onglet **Produit** et sélectionnez le modem routeur.
  3. Sur la page Web du modem routeur, cliquez sur **Micrologiciel** puis téléchargez la dernière version disponible.
  4. Pour mettre à niveau le micrologiciel, suivez les étapes décrites dans la section Administration du « Chapitre 5 : Configuration du modem routeur ADSL résidentiel sans fil G ».

13. La mise à jour du micrologiciel a échoué et/ou le voyant Power (Alimentation) clignote.

La mise à jour peut avoir échoué pour diverses raisons. Pour mettre à niveau le micrologiciel et/ou arrêter le clignotement du voyant d'alimentation, procédez comme suit :

- Si la mise à jour du micrologiciel a échoué, utilisez le programme TFTP (téléchargé avec le micrologiciel). Ouvrez le fichier PDF téléchargé avec le micrologiciel et le programme TFTP et suivez les instructions contenues dans le fichier.
- Définissez une adresse IP statique sur l'ordinateur. Reportez-vous au « Problème 1 : Je souhaite définir une adresse IP statique sur un ordinateur. » Utilisez les paramètres d'adresse IP suivants pour l'ordinateur que vous utilisez :
  Adresse IP : 192.168.1.50
  Masque de sous-réseau : 255.255.255.0
  Modem routeur : 192.168.1.1
- Effectuez la mise à jour à l'aide du programme TFTP ou l'utilitaire Web du modem routeur via l'onglet Administration.

14. Le protocole PPPoE de mon service DSL se déconnecte sans cesse.

PPPoE n'est pas réellement une connexion dédiée ou permanente. Il se peut que le FAI DSL déconnecte le service après une période d'inactivité, comme c'est le cas pour une connexion téléphonique à distance Internet.

- Une option de configuration permet de conserver la connexion « activée ». Il se peut que cela ne fonctionne pas. Dans ce cas, vous devrez rétablir la connexion de temps à autre.
  1. Pour connecter le modem routeur, ouvrez le navigateur Web et entrez http://192.168.1.1 ou l'adresse IP du modem routeur.

2. Si le système vous y invite, entrez le nom d'utilisateur et le mot de passe. Le nom d'utilisateur et le mot de passe par défaut est admin.
3. Dans l'écran Setup (Configuration), sélectionnez l'option **Keep Alive** (Activée) et définissez le délai de rappel à 20 (secondes).
4. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres). Sélectionnez l'onglet **Status** (Etat), puis cliquez sur le bouton **Connect** (Connecter).
5. Il se peut que l'état de la connexion soit défini à Connecting (Connexion en cours). Appuyez sur la touche F5 pour actualiser l'écran jusqu'à ce que l'état de la connexion soit défini à Connected (Connecté).
6. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour continuer.

- Si vous perdez de nouveau la connexion, effectuez les étapes 1 à 6 pour la rétablir.

15. Je ne parviens pas à accéder à ma messagerie électronique, au Web ou au VPN, ou je reçois des données corrompues d'Internet.

Il se peut que le paramètre d'unité de transmission maximale (MTU) nécessite une modification. Par défaut, le paramètre MTU est défini automatiquement.

- Si vous rencontrez des difficultés, procédez comme suit :
  1. Pour connecter le modem routeur, ouvrez le navigateur Web et entrez http://192.168.1.1 ou l'adresse IP du modem routeur.
  2. Si le système vous y invite, entrez le nom d'utilisateur et le mot de passe. Le nom d'utilisateur et le mot de passe par défaut est admin.
  3. Accédez à l'option MTU, puis sélectionnez **Manual** (Manuel). Dans le champ Taille, entrez 1492.
  4. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour continuer.
- Si vous rencontrez toujours des difficultés, essayez différentes valeurs de taille. Essayez la liste de valeurs suivantes (une à la fois et dans cet ordre) jusqu'à ce que le problème soit résolu :
  1462
  1400
  1362
  1300

16. Le voyant Power (Alimentation) clignote.

Le voyant Power (Alimentation) clignote lors de la mise sous tension de l'appareil. Pendant ce temps, le système démarre et vérifie les différents composants. Une fois cette opération terminée, le voyant reste allumé pour indiquer que le système fonctionne correctement. Si le voyant continue à clignoter, le système est défaillant. Essayez de démarrer le micrologiciel en attribuant une adresse IP statique à l'ordinateur, puis mettez le micrologiciel à niveau. Essayez les paramètres suivants, IP Address (Adresse IP) : 192.168.1.50 et Subnet Mask (Masque de sous-réseau) : 255.255.255.0.

17. Lorsque je spécifie une URL ou une adresse IP, j'obtiens une erreur liée à l'expiration du délai et le système m'invite à recommencer.

- Vérifiez si les autres ordinateurs fonctionnent. Si c'est le cas, assurez-vous que les paramètres IP de votre ordinateur sont corrects (IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau), Default Gateway (modem routeur par défaut) et DNS). Redémarrez l'ordinateur défaillant.
- Si l'ordinateur est configuré correctement, mais ne fonctionne toujours pas, vérifiez le modem routeur. Vérifiez qu'il est connecté et sous tension. Connectez-y vous et vérifiez ses paramètres. Si vous ne parvenez pas à vous connecter au modem routeur, vérifiez le réseau local (LAN) et les connexions d'alimentation.
- Si le modem routeur est configurée correctement, contrôlez votre connexion Internet (modem DSL/câble, etc.). Vous pouvez retirer le modem routeur pour vérifier la connexion directe.
- Configurez manuellement les paramètres TCP/IP à l'aide d'une adresse DNS fournie par votre FAI
- et assurez-vous que le navigateur est configuré pour une connexion directe et que les connexions à distance sont désactivées. Dans Internet Explorer, cliquez sur **Outils**, **Options Internet** puis sur l'onglet **Connexions**. Assurez-vous que la case à cocher **Ne jamais établir de connexion** est activée. Dans Netscape Navigator, cliquez sur **Edition**, **Préférences**, **Avancé** et **Proxies**. Assurez-vous que la case à cocher **Connexion directe à Internet** est activée

18. J'essaie d'accéder à l'utilitaire Web du modem routeur mais je ne vois pas l'écran de connexion apparaître. Un écran affichant le message « 404 Interdit » apparaît à la place.

Si vous utilisez Internet Explorer, effectuez les étapes ci-après jusqu'à ce que l'écran de connexion de l'utilitaire Web du routeur s'affiche (la même procédure est à suivre si vous utilisez Netscape) :

1. Cliquez sur **Fichier**. Assurez-vous que l'option *Travailler hors connexion* n'est PAS activée.
2. Appuyez sur **CTRL + F5**. Ce type d'actualisation forcé contraint Internet Explorer à charger les nouvelles pages Web, et non les pages mises en cache.

- Cliquez sur **Outils**. Cliquez sur **Options Internet**. Cliquez sur l'onglet **Sécurité**. Cliquez sur le bouton **Niveau par défaut**. Assurez-vous que le niveau de sécurité choisi est Moyen ou inférieur. Cliquez sur le bouton **OK**.

Questions fréquemment posées

Quel est le nombre d'adresses IP maximal que le modem routeur peut prendre en charge ?
Le modem routeur peut prendre en charge jusqu'à 253 adresses IP.

L'intercommunication IPSec est-elle prise en charge par le modem routeur ?
Oui, il s'agit d'une fonction intégrée qui est activée par défaut.

Où le modem routeur est-elle installée sur le réseau ?
Dans un environnement standard, le modem routeur est installée entre la prise murale ADSL et le réseau local (LAN).

Le modem routeur prend-elle en charge IPX ou AppleTalk ?

Non. TCP/IP est le seul protocole standard pour Internet et est devenu la norme internationale appliquée dans le cadre des communications. Les protocoles IPX (protocole de communication NetWare utilisé uniquement pour acheminer des messages d'un nœud à un autre) et AppleTalk (protocole de communication utilisé sur les réseaux Apple et Macintosh) peuvent être adoptés pour des connexions de LAN à LAN mais ne peuvent être utilisés pour relier Internet et un LAN.

La connexion LAN du modem routeur prend-elle en charge Ethernet 100 Mbit/s ?

Le modem routeur prend en charge 100 Mbit/s par l'intermédiaire d'un commutateur 10/100 Fast Ethernet à détection automatique sur le côté LAN du modem routeur.

Qu'est-ce que la technologie NAT (Network Address Translation) et quelle est sa fonction ?

La technologie NAT (Network Address Translation) permet de convertir plusieurs adresses IP d'un réseau local privé en une adresse IP publique diffusée sur Internet. Ceci ajoute un niveau de sécurité car l'adresse de l'ordinateur connecté au LAN privé ne transite jamais via Internet. En outre, la technologie NAT permet l'utilisation du modem routeur sur des comptes Internet bon marché alors que l'adresse TCP/IP est fournie le FAI. L'utilisateur peut posséder plusieurs adresses privées derrière cette adresse unique fournie par le FAI.

Le modem routeur prend-elle en charge d'autres systèmes d'exploitation que Windows 98SE, Windows Millennium, Windows 2000 ou Windows XP ?

Oui mais Linksys ne propose à l'heure actuelle aucun service de support technique réservé à l'installation, à la configuration et au dépannage de ces systèmes d'exploitation.

Le modem routeur prend-elle en charge le fichier d'envoi ICQ ?

Oui, à l'aide du correctif suivant : cliquez sur le menu ICQ -> Préférences -> onglet Connexions ->, puis activez la case à cocher indiquant que votre système se trouve derrière un pare-feu ou un serveur proxy. Dans les paramètres du pare-feu, définissez ensuite le délai à 80 secondes. L'utilisateur Internet peut alors envoyer un fichier à un autre utilisateur derrière le modem routeur.

Je souhaite définir un serveur Unreal Tournament (UT) mais les autres utilisateurs du réseau local (LAN) ne peuvent pas y accéder. Que dois-je faire ?

Si vous avez configuré un serveur Unreal Tournament, vous devez créer une adresse IP statique pour chaque ordinateur du réseau local et transférer les ports 7777, 7778, 7779, 7780, 7781 et 27900 vers l'adresse IP du serveur. Vous pouvez également utiliser une étendue de transfert de connexion comprise entre 7777 et 27900. Si vous souhaitez utiliser UT Server Admin, transférez un autre port. Le port 8080 fonctionne généralement bien mais est utilisé pour l'administration à distance. Vous devrez peut-être le désactiver.) Ensuite, dans la section [UWeb.WebServer] du fichier server.ini, définissez ListenPort à 8080 (pour qu'il corresponde au port mappé ci-dessus) et ServerName à l'adresse IP attribuée au routeur par votre FAI.

Plusieurs joueurs sur le réseau local (LAN) peuvent-ils accéder à un seul serveur de jeux et jouer simultanément à l'aide d'une seule adresse IP publique ?
Cela dépend du jeu réseau et du type de serveur de jeux que vous utilisez. Par exemple, Unreal Tournament prend en charge les connexions multiples avec une seule adresse IP publique.

Comment puis-je faire fonctionner le jeu Half-Life: Team Fortress avec le modem routeur ?
Le port client par défaut pour Half-Life est 27005. « +clientport 2700x » doit être ajouté à la ligne de commande de raccourci HL sur les ordinateurs de votre LAN, x correspondant à 6, 7, 8 et ainsi de suite. Plusieurs ordinateurs peuvent ainsi être connectés au même serveur. Il existe cependant un problème : la version 1.0.1.6 n'autorise pas plusieurs ordinateurs dotés de la même clé CD à se connecter simultanément, même s'il s'agit du même LAN (ce qui n'est pas le cas avec la version 1.0.1.3). En matière d'hébergement de jeux, il n'est pas nécessaire que le serveur HL soit dans la zone démilitarisée (DMZ). Transférez simplement le port 27015 vers l'adresse IP locale du serveur.

La page Web se bloque, les fichiers téléchargés sont corrompus et des caractères illisibles apparaissent à l'écran. Que dois-je faire ?
Forcez votre adaptateur Ethernet à 10 Mbit/s ou en mode semi-duplex, puis désactivez temporairement la fonctionnalité d'évaluation automatique de la configuration (Auto-negotiate) de votre adaptateur Ethernet (accédez au Panneau de configuration du réseau dans l'onglet Propriétés avancées de l'adaptateur Ethernet.) Assurez-vous que votre paramètre de proxy est désactivé dans le navigateur. Pour plus d'informations, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

Si tout le reste échoue au cours de l'installation, que puis-je faire ?
Réinitialisez le modem routeur en appuyant sur le bouton Reset (Réinitialisation) jusqu'à ce que le voyant Power (Alimentation) s'éteigne puis s'allume. Réinitialisez votre modem DSL en le mettant hors tension puis sous tension. Téléchargez et installez la dernière version du micrologiciel à partir du site Web international de Linksys, à l'adresse suivante : www.linksys.com/international.

Comment serai-je averti de la disponibilité des nouvelles mises à niveau du micrologiciel du modem routeur ?
Toutes les mises à niveau du micrologiciel Linksys sont disponibles sur le site Web international de Linksys (www.linksys.com/international). Vous pouvez les télécharger gratuitement. Pour mettre à niveau le micrologiciel du modem routeur, utilisez l'onglet Administration de l'utilitaire Web du modem routeur. Si la connexion Internet du modem routeur fonctionne correctement, il est inutile de télécharger une version plus récente du micrologiciel, à moins que cette version ne contienne des nouvelles fonctionnalités que vous souhaitez utiliser.

Le modem routeur fonctionne-t-elle dans un environnement Macintosh ?
Oui, mais les pages de configuration du modem routeur ne sont accessibles que par l'intermédiaire de Internet Explorer 4.0 ou Netscape Navigator 4.0 (ou version ultérieure) pour Macintosh.

Je ne parviens pas à afficher l'écran de configuration Web du modem routeur. Que puis-je faire ?
Il se peut que vous deviez supprimer les paramètres de proxy sur votre navigateur Internet (par exemple, Netscape Navigator ou Internet Explorer). Consultez la documentation de votre navigateur, Dans Internet Explorer, cliquez sur Outils, Options Internet, puis sur l'onglet Connexions. Assurez-vous que la case à cocher Ne jamais établir de connexion est activée. Dans Netscape Navigator, cliquez sur Edition, Préférences, Avancé et Proxies. Assurez-vous que la case à cocher Connexion directe à Internet est activée.

Qu'est-ce que l'hébergement DMZ ?
L'hébergement DMZ (DeMilitarized Zone) permet à une adresse IP (ordinateur) d'être exposée à Internet. Certaines applications nécessitent l'ouverture de plusieurs ports TCP/IP. Il est recommandé de configurer votre ordinateur avec une adresse IP statique si vous souhaitez utiliser l'hébergement DMZ. Pour obtenir l'adresse IP du réseau local (LAN), reportez-vous à « l'Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet ».

Si l'hébergement DMZ est utilisé, l'utilisateur exposé partage-t-il l'adresse IP publique avec le modem routeur ?
Non.

Est-ce que le modem routeur transmet les paquets PPTP ou route activement les sessions PPTP ?
Le modem routeur permet la transmission des paquets PPTP.

Le modem routeur est-elle compatible avec différentes plates-formes ?
Toutes les plates-formes qui prennent en charge Ethernet et TCP/IP sont compatibles avec le modem routeur.

Combien de ports peuvent être transférés simultanément ?
Théoriquement, le modem routeur peut établir 520 sessions simultanément mais vous ne pouvez transférer que 10 étendues de ports.

Quelles sont les fonctionnalités avancées du modem routeur ?
Les fonctionnalités avancées du modem routeur sont les paramètres sans fil avancés, les filtres, le transfert de connexion, le routage et DDNS.

Quel est le nombre de sessions VPN maximal que le modem routeur peut prendre en charge ?
Ce nombre dépend de plusieurs facteurs. Au moins une session IPSec fonctionne via le modem routeur. Néanmoins, il est possible d'ouvrir plusieurs sessions IPSec simultanément, en fonction des spécifications de vos VPN.

Comment puis-je savoir si je dispose d'une adresse IP statique ou DHCP ?
Contactez votre FAI pour obtenir cette information.

Comment puis-je faire fonctionner mIRC avec le modem routeur ?
Dans l'onglet Port Forwarding (Transfert de connexion), définissez le transfert de connexion à 113 pour l'ordinateur sur lequel vous utilisez mIRC.

Le modem routeur peut-elle être utilisée en tant que serveur DHCP ?
Oui. Le logiciel serveur DHCP est intégré au modem routeur.

Puis-je exécuter une application à partir d'un ordinateur distant via le réseau sans fil ?
Cela dépend du fait que votre application est conçue ou non pour une utilisation via un réseau. Consultez la documentation de l'application pour déterminer si elle prend en charge le fonctionnement en réseau.

Qu'est-ce que la norme IEEE 802,11g ?
Il s'agit de l'une des normes IEEE appliquées aux réseaux sans fil. La norme 802,11g permet à des appareils réseau sans fil issus de différents fabricants de communiquer, pourvu qu'ils soient conformes à cette norme. La norme 802,11g établit un taux de transfert de données maximal de 54 Mbit/s et une fréquence de fonctionnement de 2,4 GHz.

Quelles sont les fonctionnalités IEEE 802,11b et IEEE 802,11g prises en charge ?
Le produit prend en charge les fonctions IEEE 802,11b et IEEE 802,11g suivantes :

- Protocole CSMA/CA plus Acknowledge
- Itinérance multicanal
- Sélection de débit automatique
- Fonctionnalité RTS/CTS
- Fragmentation
- Gestion de l'alimentation

Il prend également en charge la technologie OFDM pour une mise en réseau 802,11g.

Qu'est-ce que le mode point à point ?
Lorsqu'un réseau sans fil est défini en mode ad hoc (point à point), les ordinateurs équipés sans fil sont configurés pour communiquer directement entre eux, point à point, sans l'intervention d'un point d'accès.

Qu'est-ce que le mode d'infrastructure ?
Lorsqu'un réseau sans fil est défini en mode d'infrastructure, le réseau sans fil est configuré pour communiquer avec un réseau via un point d'accès sans fil.

Qu'est-ce que l'itinérance ?
L'itinérance est la capacité d'un utilisateur d'ordinateur portable à communiquer en continu tout en se déplaçant dans une zone supérieure à la zone couverte par un point d'accès unique. Avant d'utiliser la fonction d'itinérance, l'ordinateur doit s'assurer que le numéro de canal est identique au point d'accès de la zone de couverture dédiée.

Pour garantir une connectivité parfaite et harmonieuse, le réseau local (LAN) sans fil doit incorporer différentes fonctions. Chaque nœud et point d'accès, par exemple, doit toujours accuser réception de chaque message. Chaque nœud doit maintenir le contact avec le réseau sans fil, même en l'absence de transmission de données. L'application simultanée de ces fonctions requiert une technologie de mise en réseau RF dynamique qui relie les points d'accès et les nœuds. Dans ce système, le nœud de l'utilisateur final recherche le meilleur accès possible au système. Il évalue tout d'abord les facteurs tels que la longueur et la qualité du signal, le chargement du message par chaque point d'accès et la distance entre chaque point d'accès et le réseau fédérateur câblé. Sur la base de ces informations, le nœud sélectionne ensuite le point d'accès correct et enregistre son adresse. Les communications entre le nœud final et l'ordinateur hôte peuvent alors être acheminées depuis ou vers le réseau fédérateur.

Lorsque l'utilisateur se déplace, l'émetteur RF du nœud final contrôle régulièrement le système afin de déterminer s'il est en contact avec le point d'accès d'origine ou s'il doit en rechercher un autre. Lorsqu'un nœud ne reçoit plus de confirmation de son point d'accès d'origine, il entreprend une nouvelle recherche. Une fois le nouveau point d'accès trouvé, il l'enregistre et le processus de communication se poursuit.

Qu'est ce que la bande ISM ?
La FCC et ses homologues internationaux ont défini une bande passante destinée à une utilisation hors licence : la bande ISM (Industrial, Scientific and Medical). Le spectre spécifique d'environ 2,4 GHz est disponible dans le monde entier. Il s'agit de la possibilité sans précédent de mettre à la disposition des utilisateurs du monde entier un système haut débit sans fil.

Qu'est-ce que la technologie d'étalement du spectre ?
La technologie d'étalement du spectre est une fréquence radio large bande développée par l'armée pour disposer d'un système fiable de transmission des communications jugées sensibles. Elle est conçue pour optimiser l'efficacité de la bande passante pour plus de fiabilité, d'intégrité et de sécurité. En d'autres termes, ce système utilise plus de bande passante que la transmission à bande étroite. Cependant, l'optimisation produit un signal qui, dans les faits, est plus important et donc plus facile à détecter, pourvu que le récepteur connaisse les paramètres du signal d'étalement du spectre transmis. Si un récepteur n'est pas défini à la bonne fréquence, le signal d'étalement du spectre est perçu comme un bruit en arrière-plan. Il existe deux autres possibilités principales avec les systèmes DSSS (Direct Sequence Spread Spectrum) et FHSS (Frequency Hopping Spread Spectrum).

Qu'est-ce que DSSS ? Qu'est-ce que FHSS ? Et quelles sont leurs différences ?

Le système FHSS (Frequency-Hopping Spread-Spectrum) utilise une porteuse à bande étroite qui modifie la fréquence en un modèle connu à la fois de l'émetteur et du récepteur. S'il est synchronisé correctement, l'effet net est le maintien d'un canal logique unique. Pour un récepteur non concerné, le signal FHSS ressemble à un bruit à impulsions courtes. Le système DSSS (Direct-Sequence Spread-Spectrum) génère un modèle de bit redondant pour chaque bit transmis. Pour ce modèle de bit, on parlera alors de puce. Plus la puce est longue, plus la probabilité de récupérer les données d'origine est grande. Même si un ou plusieurs bits de la puce sont endommagés au cours de la transmission, les techniques statistiques intégrées à la radio peuvent restaurer les données d'origine sans avoir à les retransmettre. Pour un récepteur non concerné, DSSS apparaît comme un faible bruit de transmission à large bande et est rejeté (ignoré) par la plupart des récepteurs à bande étroite.

Les informations peuvent-elles interceptées lors de leur transmission « par les airs »?

Le WLAN offre deux types de protections. Au niveau matériel, le WLAN offre une sécurité inhérente de cryptage via la technologie Direct Sequence Spread Spectrum. Au niveau logiciel, le WLAN offre une fonction de cryptage (WEP) qui améliore la sécurité et le contrôle des accès.

Qu'est-ce que WEP ?

WEP (Wired Equivalent Privacy) est un système de protection des données fondé sur un algorithme de clé partagée 64 bits ou 128 bits, conforme à la norme IEEE 802,11.

Qu'est-ce qu'une adresse MAC ?

L'adresse MAC (Media Access Control) est un numéro unique attribué par le fabricant à un périphérique réseau Ethernet, tel qu'un adaptateur réseau, qui permet au réseau de l'identifier au niveau matériel. Pour des raisons de simplicité d'utilisation, ce numéro est généralement permanent. A la différence des adresses IP qui peuvent changer dès qu'un ordinateur se connecte au réseau, l'adresse MAC d'un périphérique reste identique, ce qui en fait un identifiant réseau particulièrement fiable.

Comment puis-je réinitialiser le modem routeur ?

Appuyez pendant environ 10 secondes sur le bouton Reset (Réinitialisation) situé sur le panneau arrière du modem routeur. Cette opération réinitialise le modem routeur à ses paramètres d'usine.

Comment puis-je résoudre les problèmes liés à une perte de signal ?

Il n'est pas possible de connaître l'étendue exacte de votre réseau sans fil sans le tester. Chaque obstacle placé entre le modem routeur et un ordinateur sans fil crée une perte de signal. Les écrans de verre au plomb, le métal, les sols en béton, l'eau et les murs réduisent le signal et sa portée. Placez d'abord le modem routeur et l'ordinateur sans fil dans la même pièce et déplacez-là progressivement afin de déterminer l'étendue maximale de votre environnement.

Vous pouvez également essayer d'utiliser différents canaux et éliminer ainsi les interférences liées à un canal unique.

Mon signal est excellent mais je ne parviens pas à « voir » mon réseau.
Le WEP est probablement activé sur le modem routeur mais désactivé sur votre adaptateur sans fil (ou inversement). Vérifiez que des clés et des niveaux WEP (64 ou 128) identiques sont utilisés sur tous les nœuds de votre réseau sans fil.

Combien de canaux/fréquences sont disponibles avec le modem routeur ?
Onze canaux sont disponibles, classés de1 à 11 (en Amérique du Nord). Des canaux supplémentaires sont peut-être disponibles dans d'autres régions, en fonction des réglementations de votre région et/ou pays.

Si certaines de vos questions ne sont pas abordées dans cette annexe, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

Annexe B : Sécurité sans fil

Linksys souhaite rendre la mise en réseau sans fil aussi fiable et facile que possible. La génération actuelle de produits Linksys intègre plusieurs fonctions de sécurité réseau que vous devez cependant mettre en œuvre vous-même. Tenez compte des points suivants lors de la configuration ou de l'installation de votre réseau sans fil.

Mesures de sécurité

Cette rubrique présente une liste exhaustive des mesures de sécurité à envisager (suivez au moins les étapes 1 à 5) :

1. Modifiez le nom SSID par défaut.
2. Désactivez la fonctionnalité SSID Broadcast (Diffusion SSID).
3. Modifiez le mot de passe par défaut du compte de l'administrateur.
4. Activez la fonctionnalité MAC Address Filtering (Filtrage des adresses MAC).
5. Modifiez régulièrement le nom SSID.
6. Utilisez l'algorithme de cryptage le plus élevé possible. Utilisez la technologie WPA si elle est disponible. Notez que son utilisation peut réduire les performances de votre réseau.
7. Modifiez les clés de cryptage WEP régulièrement.

Pour obtenir des informations sur la mise en place de ces fonctions de sécurité, consultez le « chapitre 6 : Configuration du modem routeur ADSL résidentiel sans fil G ».



REMARQUE : Certaines de ces fonctions de sécurité sont disponibles uniquement via le modem routeur réseau, le routeur ou le point d'accès réseau. Pour plus d'informations, consultez la documentation du modem routeur réseau, du routeur ou du point d'accès.

Menaces liées à la sécurité des réseaux sans fil

Les réseaux sans fil sont faciles à trouver. Les pirates informatiques savent que pour se connecter à un réseau sans fil, les produits réseau sans fil doivent d'abord écouter et détecter les « messages des balises ». Ces messages sont faciles à décrypter et renferment la plupart des informations relatives au réseau, notamment son nom SSID (Service Set Identifier). Voici la procédure de protection que vous pouvez mettre en place :

Modifiez régulièrement le mot de passe de l'administrateur. Il faut savoir que les paramètres de réseau (SSID, clé WEP, etc.) des périphériques sans fil que vous utilisez sont stockés dans le micrologiciel. L'administrateur réseau est la seule personne qui puisse modifier les paramètres de réseau. Si un pirate informatique vient à connaître le mot de passe de l'administrateur, il a également la possibilité de modifier ces paramètres à sa guise. Compliquez-lui alors la tâche et rendez cette information plus difficile à obtenir. Modifiez régulièrement le mot de passe de l'administrateur.

SSID. Plusieurs éléments concernant le nom SSID sont à prendre en compte :

1. Désactiver l'option Broadcast (Diffusion).
2. Définir un SSID unique.
3. Le modifier régulièrement.

La plupart des périphériques sans fil vous donnent la possibilité de diffuser le SSID. Bien que cette option puisse s'avérer pratique, elle permet à n'importe qui de se connecter à votre réseau sans fil, y compris les pirates informatiques. Par conséquent, ne diffusez pas le nom SSID.

Les périphériques réseau sans fil possèdent un nom SSID par défaut, configuré en usine (celui de Linksys est « linksys »). Les pirates informatiques connaissent ces noms par défaut et peuvent vérifier s'ils sont utilisés sur votre réseau. Modifiez votre nom SSID, afin qu'il soit unique, tout en évitant d'en choisir un en relation avec votre société ou les périphériques réseau que vous utilisez.

Modifiez régulièrement votre nom SSID pour contraindre les pirates ayant accès à votre réseau sans fil de recommencer de zéro lors de toute tentative d'infiltration.

Adresses MAC. Activez le filtrage des adresses MAC. La fonctionnalité de filtrage des adresses MAC vous permet de réserver l'accès aux nœuds sans fil dotés de certaines adresses MAC. Le pirate informatique rencontre ainsi plus de difficultés à accéder à votre réseau au moyen d'une adresse MAC choisie au hasard.

WEP Encryption (Cryptage WEP) : Le cryptage WEP (Wired Equivalent Privacy) est souvent considéré comme la panacée en matière de protection sans fil, ce qui n'est pas toujours vrai. Cette technique fournit seulement un niveau de sécurité suffisant pour compliquer la tâche au pirate informatique.

Plusieurs moyens permettent d'optimiser l'efficacité du cryptage WEP :

1. Utilisez le niveau de cryptage le plus élevé.
2. Optez pour une authentification par clé partagée.
3. Modifiez vos clés WEP régulièrement.



IMPORTANT : Gardez toujours à l'esprit que chaque périphérique de votre réseau sans fil DOIT utiliser la même méthode et la même clé de cryptage, sans quoi votre réseau sans fil ne fonctionnera pas correctement.

WPA. Le système WPA (Wi-Fi Protected Access) offre le tout dernier et le meilleur choix standard disponible en matière de sécurité Wi-Fi. Deux modes sont disponibles : Clé pré partagée et RADIUS. Le mode Clé pré partagée vous propose deux méthodes de cryptage : La méthode TKIP (Temporal Key Integrity Protocol) qui fait appel à une méthode de cryptage renforcé et intègre un code MIC (Message Integrity Code) de protection contre les pirates et la méthode AES (Advanced Encryption System) qui procède au cryptage symétrique des données par blocs de 128 bits. Le mode RADIUS (Remote Authentication Dial-In User Service) utilise un serveur RADIUS pour authentification et application d'une méthode de cryptage TKIP, AES ou WEP dynamique.

WPA Pre-Shared Key (Clé WPA pré partagée). Si vous ne disposez pas d'un serveur RADIUS, sélectionnez le type d'algorithme (TKIP ou AES), entrez un mot de passe de 8 à 64 caractères dans le champ Pre-Shared key (Clé pré partagée), puis précisez un délai de renouvellement des clés dans l'option Group Key Renewal (Renouvellement des clés du groupe) compris entre 0 et 99 999 secondes qui indique au modem routeur ou un autre périphérique à quelle fréquence il doit changer les clés de cryptage.

WPA RADIUS. Technologie WPA utilisée conjointement avec un serveur RADIUS (ne doit être utilisé que lorsqu'un serveur RADIUS est connecté au modem routeur ou un autre périphérique). Sélectionnez d'abord le type d'algorithme WPA (**TKIP** ou **AES**). Entrez l'adresse IP et le numéro de port du serveur RADIUS, ainsi qu'une clé partagée entre le périphérique et le serveur. Précisez enfin un délai de renouvellement des clés (option Renouvellement des clés du groupe) indiquant au périphérique à quelle fréquence il doit changer les clés de cryptage.

RADIUS. Système WEP utilisé conjointement avec un serveur RADIUS (ne doit être utilisé que lorsqu'un serveur RADIUS est connecté au modem routeur ou un autre périphérique). Entrez d'abord l'adresse IP et le numéro de port du serveur RADIUS, ainsi qu'une clé partagée entre le périphérique et le serveur. Sélectionnez ensuite une clé WEP et un niveau de cryptage WEP, puis générez une clé WEP à l'aide de l'option Passphrase (Phrase mot de passe) ou entrez-la manuellement.

La mise en place d'une méthode de cryptage peut avoir un impact néfaste sur les performances de votre réseau mais reste conseillée si vous transmettez sur votre réseau des données que vous jugez confidentielles.

Ces conseils de sécurité vous permettent de conserver votre tranquillité d'esprit tout en profitant de la technologie la plus adaptée et la plus souple que Linksys vous propose.

Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet

Cette section explique comment rechercher l'adresse MAC de l'adaptateur Ethernet de votre ordinateur pour être en mesure d'utiliser la fonctionnalité de filtrage MAC du modem routeur. Vous pouvez également rechercher l'adresse IP de l'adaptateur Ethernet de votre ordinateur. Cette adresse IP est utilisée pour les fonctionnalités de filtrage, de transfert de connexion et/ou DMZ du modem routeur. Suivez la procédure décrite dans cette annexe pour rechercher l'adresse MAC ou IP de l'adaptateur sous Windows 98, Windows Me, Windows 2000 ou Windows XP.

Instructions pour Windows 98 ou Me

1. Cliquez sur **Démarrer**, puis sélectionnez **Exécuter**. Dans le champ *Ouvrir*, entrez **winipcfg.** Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK.**

2. Lorsque l'écran *Configuration IP* apparaît, sélectionnez l'adaptateur Ethernet que vous avez connecté au modem routeur à l'aide d'un câble réseau Ethernet CAT 5. Voir la figure C-1.

3. Notez l'adresse de l'adaptateur qui s'inscrit à l'écran (voir Figure C-2). Il s'agit de l'adresse MAC de votre adaptateur Ethernet. Elle apparaît sous une forme hexadécimale (série de nombres et de lettres).

   L'adresse MAC/adresse de l'adaptateur vous servira pour le filtrage MAC. L'exemple de la figure D-2 indique l'adresse MAC 00-00-00-00-00-00 de l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

   L'exemple de la figure C-2 indique l'adresse IP 192.168.1.100 de l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.



Remarque : L'adresse MAC est également appelée Adresse de l'adaptateur.



Figure C-1 : Ecran Configuration IP

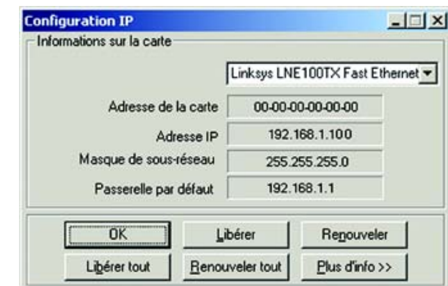


Figure C-2 : Adresse MAC/Adresse de l'adaptateur

Instructions pour Windows 2000 ou Windows XP

1. Cliquez sur **Démarrer**, puis sélectionnez **Exécuter.** Dans le champ *Ouvrir*, saisissez **cmd.** Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK.**



Remarque : L'adresse MAC est également appelée Adresse physique.

2. A l'invite de commande, entrez **ipconfig /all.** Appuyez ensuite sur la touche **Entrée.**

3. Notez l'adresse physique indiquée à l'écran (Figure C-3). Il s'agit de l'adresse MAC de votre adaptateur Ethernet. Elle apparaît sous la forme d'une série de chiffres et de lettres.

   L'adresse MAC/adresse physique vous servira pour le filtrage MAC. L'exemple de la figure C-3 indique l'adresse MAC 00-00-00-00-00-00 de l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

   L'exemple de la figure C-3 indique l'adresse IP 192.168.1.100 de l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

```
C:\WINNT\System32\cmd.exe

C:\>ipconfig /all

Configuration IP de Windows 2000

        Nom de l'hôte . . . . . . . . . . :
        Suffixe DNS principal . . . . . . :
        Type de noud. . . . . . . . . . . : Hybride
        Routage IP activé . . . . . . . . : Non
        Proxy WINS activé . . . . . . . . : Non

Ethernet carte Connexion au réseau local :

        Suffixe DNS spéc. à la connexion. :
        Description . . . . . . . . . . . : Linksys LNE100TX(V5) Fast Ethernet A
dapter
        Adresse physique. . . . . . . . . : 00-00-00-00-00-00
        DHCP activé . . . . . . . . . . . : Oui
        Autoconfiguration activée . . . . : Oui
        Adresse IP. . . . . . . . . . . . : 192.168.1.100
        Masque de sous-réseau . . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . . : 192.168.1.1
        Serveur DHCP. . . . . . . . . . . : 192.168.1.1
        Serveurs DNS. . . . . . . . . . . : 192.168.1.1
        Serveur WINS principal. . . . . . : 192.168.1.1
        Serveur WINS secondaire . . . . . :
        Bail obtenu . . . . . . . . . . . : vendredi 1 octobre 2004 12:47:43
        Bail expire . . . . . . . . . . . : lundi 4 octobre 2004 12:47:43

C:\>_
```

Figure C-3 : Adresse MAC/Adresse Physique

Annexe D : Mise à jour du micrologiciel

Pour mettre à niveau le micrologiciel du modem routeur :

1. Téléchargez le fichier de mise à jourmise à jour du micrologiciel du modem routeur depuis le site *www.linksys.com*.

2. Extrayez le fichier sur votre ordinateur.

3. Ouvrez l'utilitaire Web du modem routeur et cliquez sur l'onglet **Administration.**

4. Cliquez sur l'onglet **Firmware Upgrade** (Mise à jour du micrologiciel).

5. Cliquez sur le bouton **Browse** (Parcourir) pour rechercher le fichier extrait, puis double-cliquez sur le fichier.

6. Cliquez sur le bouton **Upgrade** (Mettre à niveau) et suivez les instructions affichées.



Figure D-1 : Mise à jour du micrologiciel

Annexe E : Glossaire

802,11b : norme de mise en réseau sans fil qui spécifie un débit de transfert de données maximum de 11 Mbit/s et une fréquence de 2,4 GHz.

802,11g : norme de mise en réseau sans fil qui spécifie un débit de transfert de données maximum de 54 Mbit/s, une fréquence de 2,4 GHz et une rétro compatibilité avec les périphériques 802,11b.

Adaptateur : périphérique ajoutant de nouvelles fonctionnalités réseau à votre ordinateur.

Adresse IP : adresse utilisée pour l'identification d'un ordinateur ou d'un périphérique sur un réseau.

Adresse IP dynamique : adresse IP attribuée provisoirement par un serveur DHCP.

Adresse IP statique : adresse fixe attribuée à un ordinateur ou un périphérique connecté à un réseau.

Adresse MAC (**M**edia **A**ccess **C**ontrol) : adresse unique qu'un fabricant attribue à chaque périphérique d'un réseau.

AES (**A**dvanced **E**ncryption **S**tandard) : méthode de sécurité utilisant un cryptage symétrique des données par blocs de 128 bits.

Bande ISM : bande radio utilisée lors de transmissions sans fil.

Bande passante : capacité de transmission d'un périphérique ou d'un réseau donné.

Base de données : ensemble de données organisées pour faciliter l'accès, la gestion et la mise à jour de leur contenu.

Bit : chiffre binaire.

Commande Finger : programme indiquant le nom associé à une adresse de messagerie.

Commutateur : 1. Commutateur de données qui relie les périphériques informatiques aux ordinateurs hôtes, permettant ainsi à de nombreux périphériques de partager un nombre limité de ports. 2. Périphérique permettant de produire, interrompre ou modifier les connexions au sein d'un circuit électrique.

Cryptage : codage de données transmises sur un réseau.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) : méthode de transfert des données adoptée pour éviter les collisions de données sur un réseau.

CTS (**C**lear **T**o **S**end) : signal émis par un périphérique sans fil pour indiquer qu'il est prêt à recevoir des données.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) : autorise l'hébergement d'un site Web, d'un serveur FTP ou d'un serveur de messagerie avec un nom de domaine fixe (par exemple www.xyz.com) et une adresse IP dynamique.

Débit - quantité de données déplacées avec succès d'un nœud à un autre dans un délai donné.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) : protocole réseau permettant aux administrateurs d'attribuer des adresses IP temporaires aux ordinateurs du réseau en louant une adresse IP à un utilisateur pour une période limitée, au lieu d'attribuer des adresses IP permanentes.

DMZ (**Dem**ilitarized **Z**one) : fonction qui supprime la protection pare-feu du routeur sur un ordinateur et le rend visible sur Internet.

DNS (**D**omain **N**ame **S**erver) : adresse IP du serveur de votre fournisseur d'accès Internet (FAI). Le système DNS permet de convertir des noms de sites Web en adresses IP.

Domaine : nom spécifique d'un réseau d'ordinateurs.

DSL (**D**igital **S**ubscriber **L**ine) : connexion haut débit toujours active par le biais des lignes téléphoniques standard.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) : transmission de fréquence qui introduit un modèle de bit redondant pour diminuer les risques de perte de données lors d'une transmission.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) : message intégré aux paquets de données et capable d'accroître l'efficacité des structures sans fil.

EAP (**E**xtensible **A**uthentication **P**rotocol) : protocole d'authentification général utilisé pour contrôler l'accès au réseau. De nombreuses méthodes d'authentification spécifiques fonctionnent ainsi.

EAP-PEAP (**E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol) : méthode d'authentification mutuelle utilisant une combinaison de certificats numériques et un autre système, comme des mots de passe.

EAP-TLS (**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity) : méthode d'authentification mutuelle utilisant des certificats numériques.

Etalement de spectre : technique de fréquence radio à large bande utilisée pour une transmission plus fiable et sécurisée des données.

Ethernet : protocole de mise en réseau qui précise la quantité de données placée ou récupérée sur un support de transmission standard.

FAI (**F**ournisseur d'**A**ccès **I**nternet) : société offrant un accès à Internet.

Fragmentation : acte de scinder un paquet en unités plus petites lors d'une transmission sur un support réseau inapte à prendre en charge la taille d'origine du paquet.

FTP (**F**ile **T**ransfer **P**rotocol) : protocole utilisé pour la transmission de fichiers sur un réseau TCP/IP.

Full Duplex : aptitude d'un périphérique réseau à recevoir et transmettre simultanément des données.

Guirlande : méthode utilisée pour connecter des périphériques en série, l'un après l'autre.

Had hoc : groupe de périphériques sans fil communiquant directement entre eux (point à point) sans l'intervention d'un point d'accès.

Haut débit : connexion Internet rapide et toujours active.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) : protocole de communication utilisé pour la connexion à des serveurs sur le World Wide Web.

Infrastructure : réseau sans fil relié à un réseau câblé via un point d'accès.

Initialiser : démarrer un périphérique et lui demander d'exécuter des instructions.

Intervalle de transmission de balise : données transmises sur un réseau sans fil en vue de le synchroniser.

IP (**I**nternet **P**rotocol) : protocole utilisé pour transmettre des données sur un réseau.

IPCONFIG : utilitaire des systèmes Windows 2000 et XP qui affiche l'adresse IP d'un périphérique réseau spécifique.

IPSec (**I**nternet **P**rotocol **Sec**urity) : protocole VPN employé pour la mise en place d'un échange sécurisé des paquets au niveau de la couche IP.

Itinérance : acte de faire passer un périphérique sans fil d'un point d'accès à un autre sans perdre la connexion.

LAN : ordinateurs ou produits mis en réseau qui constituent votre réseau local.

LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol) : méthode d'authentification mutuelle utilisant un système avec nom d'utilisateur et mot de passe.

Logiciel : instructions destinées à l'ordinateur. Série d'instructions destinée à la réalisation d'une tâche donnée appelée « programme ».

Masque de sous-réseau : code d'adresse qui détermine la taille du réseau.

Matériel : présentation physique des ordinateurs, des systèmes de télécommunication et d'autres périphériques liés aux technologies de l'information.

Mbit/s (**m**éga**bit**s par **s**econde) : soit un million de bits par seconde ; unité de mesure de transmission des données.

Micrologiciel : code de programmation qui exécute un périphérique réseau.

mIRC : programme de clavardage IRC exécuté sous Windows.

Mise à jour : acte de remplacer un logiciel ou micrologiciel existant par une nouvelle version.

Modem câble : périphérique qui relie un ordinateur au réseau de télévision câblé, ce réseau permettant à son tour de se connecter à Internet.

Multidiffusion : envoi simultané de données à un groupe de destinataires.

NAT (**N**etwork **A**ddress **T**ranslation) : la technologie NAT permet de convertir les adresses IP d'un réseau local en une adresse IP distincte sur Internet.

Navigateur : application offrant un mode d'affichage et de manipulation des informations sur le World Wide Web.

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) : protocole utilisé pour connecter des groupes Usenet sur Internet.

Nœud : liaison ou point de connexion réseau (généralement, un ordinateur ou une station de travail).

Octet : unité de données généralement équivalente à huit bits.

OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) : transmission de fréquence qui permet de séparer le flux de données en un certain nombre de flux de données à moindre débit, transmis ensuite en parallèle pour diminuer les risques de perte de données lors d'une transmission.

Paquet : unité de données transmises sur un réseau.

Pare-feu : ensemble de programmes associés situés sur un serveur de modem routeur de réseau protégeant les ressources d'un réseau des utilisateurs d'autres réseaux.

Pare-feu SPI (**S**tateful **P**acket **I**nspection) : technologie inspectant les paquets d'informations entrants avant de les autoriser à pénétrer le réseau.

Passerelle : périphérique permettant de relier entre eux des réseaux dotés de protocoles de communication incompatibles.

Passerelle par défaut : périphérique utilisé pour transférer un trafic de données Internet depuis votre réseau local.

PEAP (**P**rotected **E**xtensible **A**uthentication **P**rotocol) : méthode d'authentification mutuelle utilisant une combinaison de certificats numériques et un autre système, comme des mots de passe.

Phrase mot de passe : utilisée comme un mot de passe, une phrase mot de passe simplifie le processus de cryptage WEP en générant automatiquement les clés de cryptage WEP des produits Linksys.

Ping (**P**acket **IN**ternet **G**roper) : utilitaire Internet utilisé pour déterminer si une adresse IP particulière est en ligne.

Point d'accès : périphérique permettant aux ordinateurs et aux autres périphériques sans fil de communiquer avec un réseau câblé. Il sert également à étendre la portée d'un réseau sans fil.

Pont : périphérique reliant différents réseaux.

POP3 (**P**ost **O**ffice **P**rotocol **3**) : serveur de messagerie standard couramment utilisé sur Internet.

Port : point de connexion sur un ordinateur ou un périphérique réseau utilisé pour le branchement à un câble ou un adaptateur.

Power **o**ver **E**thernet (**PoE**) : technologie permettant à un câble réseau Ethernet de transiter des données et l'alimentation.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) : type de connexion haut débit qui permet l'authentification (nom d'utilisateur et mot de passe) et l'acheminement des données.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) : protocole VPN qui permet au protocole PPP (Point to Point Protocol) de traverser un réseau IP. Il est également utilisé comme type de connexion haut débit en Europe.

Préambule : partie du signal sans fil chargée de synchroniser le trafic réseau.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) : protocole utilisant un serveur d'authentification pour contrôler l'accès au réseau.

Réseau : plusieurs ordinateurs ou périphériques reliés entre eux dans le but de partager et de stocker des données et/ou de permettre la transmission de données entre des utilisateurs.

Réseau fédérateur : partie d'un réseau qui permet de relier la plupart des systèmes et des réseaux entre eux et de gérer la majorité des données.

RJ-45 (**R**egistered **J**ack**-45)** : connecteur Ethernet pouvant accueillir jusqu'à huit broches.

Routage statique : transfert de données sur un réseau par une voie fixe.

Routeur : périphérique de mise en réseau qui relie entre eux plusieurs ordinateurs.

RTS (**R**equest **T**o **S**end) : méthode de mise en réseau consistant à coordonner des paquets importants par le biais du paramètre RTS Threshold (Seuil RTS).

Semi-duplex : transmission de données pouvant survenir dans deux directions sur une ligne unique, mais une direction à la fois.

Serveur : tout ordinateur dont le rôle sur un réseau est de fournir aux utilisateurs un accès à des fichiers, des imprimantes, des outils de communication et d'autres services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) : protocole de messagerie standard utilisé sur Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) : protocole très répandu de contrôle et d'administration de réseau.

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) : segment de marché des professionnels qui travaillent à domicile ou dans des petits bureaux.

SSID (**S**ervice **S**et **ID**entifier) : nom de votre réseau sans fil.

Tampon : zone de mémoire partagée ou affectée utilisée pour prendre en charge et coordonner plusieurs activités informatiques et réseau de façon à ce qu'une activité ne soit pas interrompue par une autre.

TCP (**T**ransmission **C**ontrol **P**rotocol) : protocole réseau de transmission de données exigeant la validation de la personne à qui elles sont destinées.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) : désigne un ensemble d'instructions (ou protocole) que tous les ordinateurs suivent pour communiquer sur un réseau.

Téléchargement : réception d'un fichier transmis sur un réseau.

Telnet : commande utilisateur et protocole TCP/IP utilisés pour l'accès à des ordinateurs distants.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) : version du protocole FTP TCP/IP n'offrant aucune fonction de répertoire ou de mot de passe.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) : protocole de cryptage sans fil qui fournit des clés de cryptage dynamiques pour chaque paquet transmis.

Topologie : configuration physique d'un réseau.

UDP (**U**ser **D**atagram **P**rotocol) : protocole réseau de transmission de données n'exigeant aucune validation de la personne à qui elles sont destinées.

URL (**U**niform **R**esource **L**ocator) : adresse d'un fichier situé sur Internet.

Vitesse de transmission : taux de transmission.

VPN (**V**irtual **P**rivate **N**etwork) : mesure de sécurité visant à protéger des données lorsqu'elles quittent un réseau et s'acheminent vers un autre via Internet.

WAN (**W**ide **A**rea **N**etwork) : Internet.

WEP (**W**ired **E**quivalent **P**rivacy) : méthode permettant de crypter des données transmises sur un réseau sans fil pour une sécurité accrue.

WINIPCFG : utilitaire Windows 98 et Windows Me qui affiche l'adresse IP d'un périphérique réseau spécifique.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) : groupe d'ordinateurs et de périphériques associés qui communiquent entre eux sans fil.

WPA (**W**i-Fi **P**rotected **A**ccess) : protocole de sécurité sans fil faisant appel au cryptage TKIP (Temporal Key Integrity Protocol) et pouvant être utilisé en association avec un serveur RADIUS.

Annexe F : Réglementation

Ce produit répond aux exigences essentielles de la directive européenne 1999/5/EC et est destiné à tous les pays européens (des restrictions peuvent s'appliquer).

Informations de conformité pour les produits sans fil 2,4 GHz concernant l'Union européenne et les autres pays suivant la directive européenne 1999/5/EC (R&TTE)

Déclaration de conformité concernant la directive européenne 1995/5/CE (R&TTE)

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

REMARQUE : Si vous avez besoin de documentation technique, reportez-vous à la section « Comment accéder aux documents techniques depuis l'adresse www.linksys.com/international » pour plus d'informations.

Les normes suivantes ont été appliquées lors de l'appréciation du produit avec les normes de la directive 1999/5/EC :

- Radio : EN 300 328
- Compatibilité électromagnétique : EN 301 489-1, EN 301 489-17
- Sécurité : EN 60950

Marquage CE

Pour les produits Linksys sans fil B et G, le marquage CE, le numéro de l'organisme notifié (le cas échéant) et l'identifiant de classe 2 suivants sont ajoutés à l'équipement.

CE 0560 ⓘ ou CE 0678 ⓘ ou CE ⓘ

Vérifiez l'étiquette CE sur le produit pour déterminer quel numéro d'organisme notifié a été pris en compte pendant l'appréciation.

Restrictions nationales

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'Union européenne (et dans tous les pays ayant transposé la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous :

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

Belgique

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

France

In case the product is used outdoors, the output power is restricted in some parts of the band. See Table 1 or check http://www.art-telecom.fr/ for more details.

Dans le cas d’une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous au tableau 1 ou visitez le site Web http://www.art-telecom.fr/ pour de plus amples détails.

Table 1: Niveaux de puissance en vigueur en France

Emplacement	**Bande de fréquences (MHz)**	**Puissance (PIRE)**
Utilisation en intérieur (pas de restrictions)	2400-2483.5	100 mW (20 dBm)
Utilisation en extérieur	2400-2454 2454-2483.5	100 mW (20 dBm) 10 mW (10 dBm)

Italie

Ce produit est conforme à National Radio Interface et aux recommandations définies dans la National Frequency Allocation Table de l'Italie. L'utilisation de ce produit LAN 2,4 GHz est soumis à une autorisation générale, sauf s'il est utilisé dans les limites de la propriété de l'utilisateur. Consultez le site http://www.comunicazioni.it/it/ pour de plus amples détails.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all’interno del proprio fondo, l’utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una “Autorizzazione Generale”. Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Restrictions d'utilisation du produit

Ce produit est conçu pour une utilisation intérieure uniquement. L'utilisation en extérieur n'est pas recommandée.

Ce produit est conçu pour une utilisation avec une ou plusieurs antennes intégrales ou externes (dédiées). L'utilisation d'antennes non dédiées ou tierces n'est pas recommandée et n'est pas prise en charge par Linksys.

Sortie de votre périphérique

Afin de respecter les réglementations de votre pays, vous devrez peut-être modifier la sortie de votre périphérique sans fil. Reportez-vous à la section consacrée à votre périphérique.

Remarque : Le paramètre de sortie n'est peut être pas disponible sur tous les produits sans fil. Pour de plus amples informations, reportez-vous à la documentation sur le CD du produit ou visitez le site http://www.linksys.com/international.

Adaptateurs sans fil

La sortie des adaptateurs sans fil est définie à 100 % par défaut. La sortie maximale de chaque adaptateur ne dépasse pas 20 dBm (100 mW). Elle est généralement de 18 dBm (64 mW) ou inférieure. Si vous avez besoin de modifier la sortie de votre adaptateur sans fil, suivez les instructions correspondantes au système d'exploitation de votre ordinateur :

Windows XP

1. Cliquez deux fois sur l'icône **Sans fil** dans la barre d'état système de votre bureau.
2. Ouvrez la fenêtre *Connexion réseau sans fil*.
3. Cliquez sur le bouton **Propriétés.**
4. Sélectionnez l'onglet **Général** et cliquez sur le bouton **Configurer**.
5. Dans la fenêtre *Propriétés*, cliquez sur l'onglet **Avancé**.
6. Sélectionnez **Sortie.**
7. A partir du menu déroulant à droite, sélectionnez le pourcentage de sortie de l'adaptateur sans fil.

Windows 2000

1. Ouvrez le **Panneau de configuration**.
2. Cliquez deux fois sur **Connexions réseau et accès à distance**.
3. Sélectionnez votre connexion sans fil actuelle et sélectionnez **Propriétés**.
4. Dans l'écran *Propriétés*, cliquez sur le bouton **Configurer.**
5. Cliquez sur l'onglet **Avancé** et sélectionnez **Sortie.**
6. A partir du menu déroulant à droite, sélectionnez le paramètre de puissance de l'adaptateur sans fil.

Si vous utilisez Windows Me ou 98, reportez-vous à l'aide de Windows pour obtenir des instructions sur le mode d'accès des paramètres avancés d'un adaptateur réseau.

Points d'accès, routeurs ou autres produits sans fil

Si vous utilisez un point d'accès, un routeur ou un autre produit sans fil, utilisez son utilitaire Web pour configurer son paramètre de sortie (reportez-vous à la documentation du produit pour obtenir davantage d'informations).

Documents techniques disponibles sur le site www.linksys.com/international

Pour accéder aux documents techniques, procédez comme suit :

1. Accédez à la page http://www.linksys.com/international.
2. Cliquez sur votre région de résidence.
3. Cliquez sur le nom du pays de votre résidence.
4. Cliquez sur **Produit**.
5. Cliquez sur la catégorie de produit appropriée.
6. Sélectionnez un produit.
7. Cliquez sur le type de documentation que vous souhaitez. Le document va s'ouvrir automatiquement au format PDF.

Remarque : Si vous avez des questions au sujet de la conformité de ces produits ou que vous ne trouvez pas les informations que vous recherchez, contactez votre bureau de vente local. Visitez le site http://www.linksys.com/international pour de plus amples informations.

AVERTISSEMENTS RELATIFS A LA SECURITE

Avertissement : Afin de réduire les risques d'incendies, utilisez uniquement des câbles téléphoniques No.26 AWG (ou de diamètre supérieur).

N'utilisez pas le produit à proximité de l'eau, par exemple, sur un sol humide ou près d'une piscine.

Evitez d'utiliser ce produit pendant un orage.

Annexe G : Informations de garantie

Linksys garantit que vos produits Linksys seront, pour l'essentiel, exempts de vices matériels et de fabrication, sous réserve d'une utilisation normale, pendant une période de trois années consécutives (« Période de garantie »). Votre unique recours et l'entière responsabilité de Linksys seront limités, au choix de Linksys, soit à la réparation ou au remplacement du produit, soit au remboursement du prix à l'achat moins les remises effectuées. Cette garantie limitée concerne uniquement l'acheteur d'origine.

Si ce produit devait s'avérer défectueux pendant cette période de garantie, contactez le support technique de Linksys pour obtenir, si besoin est, un numéro d'autorisation de retour. N'OUBLIEZ PAS DE CONSERVER VOTRE PREUVE D'ACHAT A PORTEE DE MAIN LORS DE TOUT CONTACT TELEPHONIQUE. Si Linksys vous demande de retourner le produit, indiquez lisiblement le numéro d'autorisation de retour à l'extérieur de l'emballage et joignez-y une copie de l'original de votre preuve d'achat. TOUTE DEMANDE DE RETOUR NE PEUT ETRE TRAITEE EN L'ABSENCE D'UNE PREUVE D'ACHAT. Les frais d'expédition des produits défectueux à Linksys sont à votre charge. Linksys prend uniquement en charge les envois via UPS Ground de Linksys chez vous. Les frais d'envoi restent à la charge des clients implantés en dehors des Etats-Unis et du Canada.

TOUTES LES GARANTIES IMPLICITES ET CONDITIONS DE VALEUR MARCHANDE OU D'ADEQUATION A UN USAGE PARTICULIER SONT LIMITEES A LA DUREE DE LA PERIODE DE GARANTIE. TOUTES LES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES IMPLICITES OU EXPLICITES, Y COMPRIS TOUTE GARANTIE IMPLICITE DE NON-CONTREFACON SONT DEMENTIES. Certaines juridictions n'autorisent pas les restrictions relatives à la durée d'une garantie implicite. Par conséquent, la restriction susmentionnée peut ne pas s'appliquer dans votre cas. Cette garantie vous accorde des droits spécifiques. Vous pouvez avoir d'autres droits qui varient en fonction des juridictions.

Cette garantie ne s'applique pas si le produit (a) a été modifié, sauf si cette modification est le fait de Linksys, (b) n'a pas été installé, exploité, réparé ou entretenu conformément aux instructions fournies pas Linksys ou (c) a été altéré suite à une charge physique ou électrique anormale, un usage inadapté du produit, une négligence ou un accident. De plus, en raison du développement permanent de nouvelles techniques visant à infiltrer et attaquer les réseaux, Linksys ne garantit pas que le présent produit est protégé contre toute intrusion ou attaque dont vous feriez l'objet.

CONFORMEMENT A LA LOI ET INDEPENDAMMENT DE LA THEORIE SUR LES RESPONSABILITES, LINKSYS NE POURRA EN AUCUN CAS ETRE TENU RESPONSABLE DES PERTES DE DONNEES, DE REVENUS OU DE BENEFICES OU DES DOMMAGES SPECIAUX, INDIRECTS, CONSECUTIFS, ACCIDENTELS OU DISSUASIFS (Y COMPRIS LES ACTES DE NEGLIGENCE) LIES OU NON LIES A L'UTILISATION OU A L'INCAPACITE A UTILISER LE PRODUIT (Y COMPRIS TOUS LES LOGICIELS), MEME SI LINKSYS A ETE AVERTI DE LA POSSIBILITE DE TELS DOMMAGES. LA RESPONSABILITE DE LINKSYS NE DEPASSE EN AUCUN CAS LE MONTANT REGLE PAR VOS SOINS POUR LE PRODUIT. Les restrictions susmentionnées s'appliqueront même si toutes les garanties ou les recours stipulés dans le présent Contrat ne remplissent pas leur fonction principale. Certaines juridictions n'autorisent pas l'exclusion ou la limitation des dommages accessoires ou fortuits, de telle sorte que la limitation ou l'exclusion susmentionnée peut ne pas vous être applicable.

Cette garantie est valide et peut ne s'appliquer que dans le pays d'acquisition du produit.

Veuillez envoyer toutes vos demandes de renseignement à l'adresse suivante : Linksys, P.O. Box 18558, Irvine, CA 92623.

Annexe H : Spécifications

Référence du modèle	WAG354G
Normes	IEEE 802,11g, IEEE 802,11b, IEEE 802.3, IEEE 802,3u, G.992,1 (G.dmt), G.992,2 (G.lite), G.992.3, G.992.5, T1.413i2
Ports	Power (Alimentation), ADSL, Ethernet (1-4)
Boutons	Un bouton Reset (Réinitialiser)
Type de câblage	UTP CAT 5
Voyants	Power (Alimentation), Wireless (Sans fil), Ethernet (1-4), DSL, Internet
Puissance à l'émission	18 dBm
Canaux	13 (utilisables dans la plupart des pays de l'Union Européenne)
Prise en charge UPnP (possible/certifiée)	Possible
Fonctions de sécurité	Configuration protégée par mot de passe pour l'accès Web Authentifications PAP et CHAP Prévention des attaques DoS (Denial of Service) Filtrage des URL et blocage des mots-clés, de Java, d'ActiveX, de Proxy et des cookies Filtre ToD (accès aux blocs selon le moment) Intercommunications VPN pour IPSec, protocoles PPTP et L2TP

	WEP 128 bits, 64 bits avec génération de clé WEP/phrase mot de passe SSID Broadcast Disable (Désactivation de la diffusion SSID) Restriction d'accès par les adresses MAC et IP
Configuration binaire de la clé WEP	64/128 bits
Dimensions	140 x 140 x 27 mm
Poids	0,3 kg
Alimentation	12 Vcc 1 A
Certifications	CE
Operating Temp.	0º à 40º C
Storage Temp.	-20º à 70ºC
Humidité en fonctionnement	10 à 85 %, non condensée
Humidité de stockage	5 à 95 %, non condensée

Annexe I : Contacts

Besoin de contacter Linksys ?
Consultez notre site Web pour obtenir des informations sur les derniers produits et les mises à jour disponibles pour vos produits existants à l'adresse suivante :
http://www.linksys.com/international

Si vous rencontrez des problèmes avec un produit Linksys, adressez-nous un courrier électronique et envoyez-le au service Support technique du pays où vous résidez :

Europe	Adresse électronique
Allemagne	support.de@linksys.com
Autriche	support.at@linksys.com
Belgique	support.be@linksys.com
Danemark	support.dk@linksys.com
Espagne	support.es@linksys.com
France	support.fr@linksys.com
Italie	support.it@linksys.com
Norvège	support.no@linksys.com
Pays-Bas	support.nl@linksys.com
Portugal	support.pt@linksys.com
Royaume-Uni et Irlande	support.uk@linksys.com
Suède	support.se@linksys.com
Suisse	support.ch@linksys.com

Hors Europe	Adresse électronique
Amérique Latine	support.la@linksys.com
Etats-Unis et Canada	support@linksys.com

LINKSYS®

A Division of Cisco Systems, Inc.



2,4 GHz 802.11g **Wireless-G**



ADSL-gateway för hemmet

Användarhandbok



Modellnummer **WAG354G (SE)**

Copyright och varumärken

Så här använder du handboken

Din handbok till Wireless-G ADSL-gateway för hemmet gör nätverksanvändning med gatewayen enklare än någonsin. Titta efter följande när du läser användarhandboken:



Bocken betyder att det står något extra viktigt som du bör uppmärksamma när du använder gatewayen.



Utropstecknet står för en varning för något som kan skada din egendom eller gatewayen.



Frågetecknet påminner dig om något du måste göra när du använder gatewayen.

Förutom dessa symboler finns det definitioner av tekniska termer som presenteras på följande sätt:

ord: *definition.*

Alla bilder har ett bildnummer och en beskrivning som ser ut så här:

Bild 0-1: Exempel på bildbeskrivning

Bildnummer och beskrivningar finns också i avsnittet "Bilder" i innehållsförteckningen.

WAG354G-SE-UG-50315B JL

Innehåll

Bilder

Kapitel 1: Introduktion

Välkommen

Tack för att du valde Wireless-G ADSL-gateway för hemmet. Den här gatewayen ger dina datorer tillgång till en snabb Internet-anslutning och resurser som filer och skrivare. Eftersom gatewayen är trådlös kan du dela Internet-uppkopplingen både över det trådanslutna- och det trådlösa nätverket med en hastighet upp till 11 Mbit/s för Wireless-B eller upp till 54 Mbit/s för Wireless-G.

Hur kan gatewayen klara allt detta? Anslut Internet-uppkopplingen och alla dina datorer och kringutrustning till gatewayen och låt den sedan styra och kontrollera kommunikationen i nätverket.

För att skydda dina data och din integritet har gatewayen en avancerad brandvägg som håller Internet-inkräktare borta. Du kan skydda de trådlösa överföringarna genom kraftfull datakryptering. Dessutom kan du skydda familjen med barnlåsfunktioner som tidsbegränsad Internet-åtkomst och blockerade nyckelord. Du konfigurerar gatewayens inställningar via det lättanvända webbaserade verktyget.

Men vad betyder allt detta?

Nätverk är användbara verktyg för att t.ex. dela Internet-åtkomst och datorresurser. Du kan skriva ut på en skrivare från flera datorer och komma åt data på en annan dators hårddisk. Nätverk används även när man spelar videospel med flera användare. Nätverk är alltså inte bara användbara i hem och på kontor, de kan även vara en källa till nöje.

Datorer anslutna till ett nätverk via kablar kallas för ett LAN (Local Area Network). De ansluts med Ethernet-kablar - det är därför nätverket kallas trådanslutet. Datorer med trådlösa nätverkskort eller nätverksadaptrar kan kommunicera utan klumpiga kablar. Genom att dela samma trådlösa inställningar inom överföringsräckvidden, utgör de ett trådlöst nätverk. Detta kallas ibland ett WLAN (Wireless Local Area Network). Eftersom gatewayen har trådlösa funktioner kan den fungera som en brygga mellan dina trådanslutna- och trådlösa nätverk och låta dem kommunicera med varandra.

När nätverken är anslutna, kabel, trådlöst och Internet, kan du börja dela filer och Internet-uppkoppling – och till och med spela spel. Och hela tiden skyddar Wireless-G ADSL-gateway för hemmet dina nätverk från obehörig åtkomst och ovälkomna användare.

Linksys rekommenderar att du använder konfigurationsskivan för den första installationen av gatewayen. Om du inte vill köra konfigurationsguiden på cd-skivan följer du anvisningarna i denna handbok som hjälper dig ansluta gatewayen och konfigurera den som en brygga mellan de olika nätverken. Dessa anvisningar bör vara allt du behöver för att få ut det mesta möjliga av Wireless-G ADSL-gateway för hemmet.

***wpa** (wi-fi protected access): ett trådlöst säkerhetsprotokoll med TKIP-kryptering (Temporal Key Integrity Protocol) som kan användas tillsammans med en RADIUS-server.*

***spi-brandvägg** (stateful packet inspection): en teknik som inspekterar inkommande paket med data innan de får tillgång till nätverket.*

***brandvägg**: Säkerhetsåtgärder som skyddar resurserna från intrång i ett lokalt nätverk.*

***nat** (network address translation): NAT-tekniken översätter IP-adresser i ett lokalt nätverk till en annan IP-adress för Internet.*

***nätverk**: en serie datorer eller enheter anslutna i syfte att dela data, lagring och/eller överföring mellan användare*

***lan** (local area network): De datorer och nätverksprodukter som utgör nätverket i hemmet eller på kontoret.*

Vad innehåller denna användarhandbok?

Användarhandboken täcker konfigurationen och användningen av Wireless-G ADSL-gateway för hemmet.

- Kapitel 1: Introduktion
  Det här kapitlet beskriver användningen av Wireless-G ADSL-gateway för hemmet och denna användarhandbok.
- Kapitel 2: Planera nätverket
  Det här kapitlet beskriver grunderna i nätverk.
- Kapitel 3: Lära känna Wireless-G ADSL-gateway för hemmet
  I det här kapitlet beskrivs gatewayens fysiska egenskaper.
- Kapitel 4: Ansluta Wireless-G ADSL-gateway för hemmet
  I det här kapitlet förklaras hur du ansluter gatewayen till nätverket.
- Kapitel 5: Konfigurera Wireless-G ADSL-gateway för hemmet
  I det här kapitlet beskrivs hur du konfigurerar gatewayens inställningar från det webbaserade verktyget.
- Bilaga A: Felsökning
  I den här bilagan beskrivs några problem och lösningar samt vanliga frågor rörande installation och användning av Wireless-G ADSL-gateway för hemmet.
- Bilaga B: Trådlös säkerhet
  I den här bilagan förklaras riskerna med trådlösa nätverk och några lösningar som minskar riskerna.
- Bilaga C: Hitta MAC-adress och IP-adress för Ethernet-adaptern
  I den här bilagan beskrivs hur du hittar MAC-adressen för datorns Ethernet-adapter, så att du kan använda gatewayens funktion för MAC-filtrering och/eller funktionen för kloning av MAC-adress.
- Bilaga D: Uppgradera den fasta programvaran
  I den här bilagan förklaras hur du uppgraderar gatewayens fasta programvara om det skulle bli nödvändigt.
- Bilaga E: Ordlista
  I den här bilagan finns en kort ordlista med termer som ofta används i nätverkssammanhang.
- Bilaga F: Information om regler
  I den här bilagan anges information om regler rörande gatewayen.
- Bilaga G: Garantiinformation
  I den här bilagan anges gatewayens garantiinformation.

- Bilaga H: Specifikationer
  I den här bilagan finns gatewayens tekniska specifikationer.

- Bilaga I: Kontaktinformation
  I den här bilagan anges kontaktinformation för olika Linksys-resurser, t.ex. teknisk support.

Kapitel 2: Planera nätverket

Gatewayens funktioner

En gateway är en nätverksenhet som ansluter två nätverk till varandra.

Här ansluter gatewayen ditt lokala nätverk (LAN), eller grupper av datorer i hemmet eller på kontoret, till Internet. Gatewayen bearbetar och reglerar datainformationen som färdas mellan dessa två nätverk.

Gatewayens NAT-funktion skyddar nätverket med datorer så att användare på den offentliga, Internet-sidan, inte kan "se" dina datorer. Det är så här som ditt nätverk förblir privat. Gatewayen skyddar nätverket genom att inspektera alla paket som kommer in genom Internet-porten innan de levereras till rätt dator i nätverket. Gatewayen inspekterar Internet-porttjänster som webbservern, ftp-servern eller andra Internet-tillämpningar, och vidarebefordrar sedan, om den tillåts, paketet till rätt dator på LAN-sidan.

Kom ihåg att gatewayens portar ansluter till två sidor. LAN-portarna ansluter till LAN och ADSL-porten till Internet. LAN-portarna överför data med 10/100 Mbit/s.



Bild 2-1: Nätverk:

ip *(internet protocol): ett protokoll som används för att skicka data över ett nätverk*

IP-adresser

Vad är en IP-adress?

IP står för Internet Protocol. Alla enheter i ett IP-baserat nätverk, inklusive datorer, skrivarservrar och gatewayer, kräver en IP-adress för att identifiera "plats" eller "adress" i nätverket. Detta gäller både Internet- och LAN-anslutningar. Nätverksenheter kan tilldelas IP-adresser på två sätt. Du kan tilldela statiska IP-adresser eller låta gatewayen tilldela IP-adresser dynamiskt.

Statiska IP-adresser

En statisk IP-adress är en fast IP-adress som du tilldelar manuellt till en dator eller annan enhet i nätverket. Eftersom en statisk IP-adress är giltig tills du avaktiverar den, garanterar statisk tilldelning av IP-adresser att enheten alltid har samma IP-adress tills du ändrar den. Statiska IP-adresser måste vara unika och används vanligen för nätverksenheter som serverdatorer eller skrivarservrar.



OBS! Eftersom gatewayen är en enhet som ansluter två nätverk, behöver den två IP-adresser - en för det lokala nätverket och en för Internet. I den här användarhandboken används hänvisningar till "Internet IP-adress" och "LAN IP-adress".

Eftersom gatewayen använder NAT-teknik, är den enda IP-adress som syns från Internet för hela ditt nätverk, gatewayens Internet IP-adress. Det går även att blockera denna Internet IP-adress så att gatewayen och nätverket blir osynliga för Internet - se beskrivningen av blockering av WAN-begäran i avsnittet Säkerhet i "Kapitel 5: Konfigurera Wireless-G ADS-gateway för hemmet".

Eftersom du använder gatewayen till att dela din DSL-baserade Internet-anslutning, måste du kontakta din Internet-leverantör och fråga om de tilldelat ditt konto en statisk IP-adress. I så fall behöver du den statiska IP-adressen när du konfigurerar gatewayen. Du kan få denna information från Internet-leverantören.

Dynamiska IP-adresser

En dynamisk IP-adress tilldelas automatiskt till en enhet i nätverket, t.ex. datorer och skrivarservrar. Dessa IP-adresser kallas "dynamiska" eftersom de bara tillfälligt tilldelas till en dator eller enhet. Efter en viss tidsperiod förfaller de och kan därför ändras. Om en dator loggar in på nätverket (eller Internet) och dess dynamiska IP-adress har förfallit, tilldelas den en ny dynamisk IP-adress av DHCP-servern.

DHCP-servrar (Dynamic Host Configuration Protocol)

Datorer och andra nätverksenheter med dynamisk tilldelning av IP-adresser tilldelas en ny IP-adress av en DHCP-server. Datorn eller nätverksenheten som erhåller en IP-adress kallas för DHCP-klienten. DHCP frigör dig från arbetet att tilldela IP-adresser manuellt varje gång en ny användare läggs till i nätverket.

En DHCP-server kan vara en tilldelad dator i nätverket eller en annan nätverksenhet, t.ex. gatewayen. Som standard är gatewayens DHCP-serverfunktion aktiverad.

Om du redan har en DHCP-server igång i nätverket måste du avaktivera en av de två DHCP-servrarna. Om du har flera DHCP-servrar igång samtidigt i nätverket kommer du att få nätverksfel, t.ex. IP-adresser som ligger i konflikt med varandra. Anvisningar för hur du avaktiverar DHCP på gatewayen finns i avsnittet DHCP i "Kapitel 5: Konfigurera Wireless-G ADSL-gateway för hemmet".

Kapitel 3: Börja lära känna Wireless-G ADSL-gateway för hemmet

Portar och återställningsknapp på sidopanelen

Gatewayens portar och återställningsknapp finns på sidopanelen.

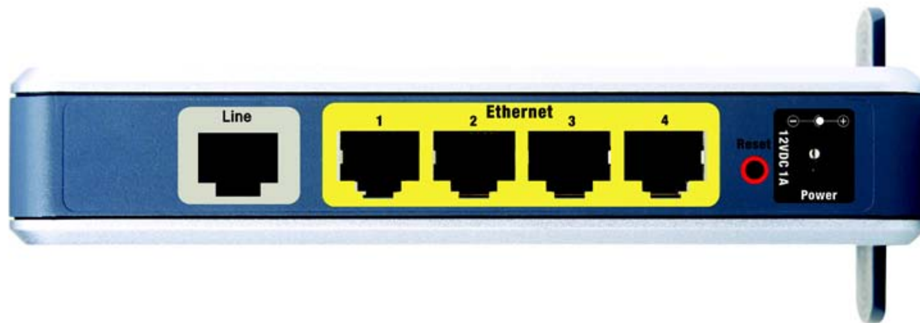


Bild 3-1: Portar och återställningsknapp på sidopanelen

Line	**Line-**porten ansluts till ADSL-linjen.
Ethernet (1-4)	**Ethernet-**portarna ansluts till dina datorer och andra nätverksenheter.
Reset	Du kan återställa gatewayen till fabriksinställningar på två sätt. Antingen håller in knappen **Reset** (Återställ) i ca. tio sekunder eller så återställer du dem från dialogrutan *Factory Defaults* (Fabriksinställningar) på fliken Administration i gatewayens webbaserade konfigurationsverktyg.
Power	Till **Power-**porten ansluter du strömförsörjningsadaptern.



VIKTIGT! Om du återställer gatewayen till fabriksinställningarna raderas alla dina inställningar (även dem för Internet-anslutning och trådlösa anslutningar) och ersätts med fabriksinställningarna. Återställ inte gatewayen om du vill behålla dessa inställningar.

Lysdioder på sidopanelen

Gatewayens lysdioder som anger nätverksaktivitet sitter på den andra sidopanelen.



Bild 3-2: Lysdioder på sidopanelen

POWER Grön. **POWER**-lysdioden lyser när gatewayen är påslagen.

WIRELESS Grön. **WIRELESS**-lysdioden lyser när det finns en trådlös anslutning. Om lysdioden blinkar skickar eller tar gatewayen aktivt emot data till eller från en av enheterna i nätverket.

ETHERNET (1-4) Grön. **ETHERNET**-lysdioderna har två syften. Om lysdioden lyser med fast sken är gatewayen ansluten till en enhet via LAN-porten. Om lysdioden blinkar är det en indikation på nätverksaktivitet.

DSL Grön. **DSL**-lysdioden lyser när det finns en DSL-anslutning. Lysdioden blinkar under tiden som gatewayen försöker upprätta ADSL-anslutningen.

INTERNET Grön. INTERNET-lysdioden lyser med grönt sken när en Internet-anslutning till Internet-leverantören (ISP) har upprättats. INTERNET-lysdioden lyser med rött sken när anslutningen till Internet-leverantören misslyckas.

Toppanelen

Gatewayen levereras med en inbyggd antenn, men du kan ansluta en tillvalsantenn om du vill. (Obs! Antennen finns för närvarande inte i Europa.) Linksys 5dBi högeffektsantenn för SMA-anslutningar (modellnummer: HGA5S) finns tillgänglig för längre räckvidd. Gatewayens SMA-port för tillvalsantennen sitter på toppanelen. Om du vill få tillgång till SMA-porten trycker du på fliken. Du ansluter antennen genom att sätta in den nedre delen i SMA-porten och sedan dra åt den medurs för hand.



Bild 3-3: Toppanel

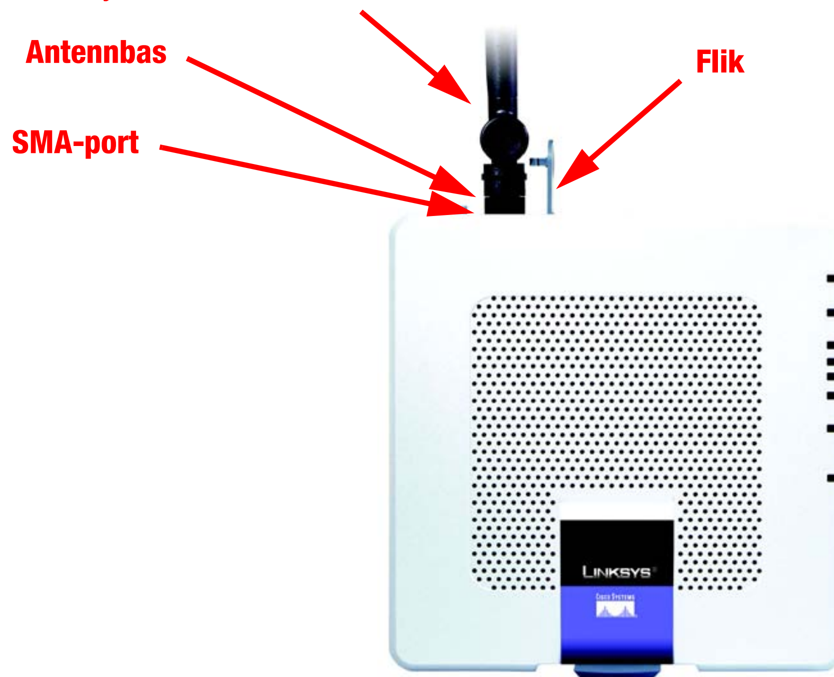


Bild 3-4: Toppanel med tillvalsantenn

Bottenpanelen

Gatewayen har ett inbyggt ställ. Om du ställer gatewayen på en plan yta kan du låta stället vara infällt. Om du däremot vill att gatewayen ska stå upp vrider du stället 90° och ställer sedan gatewayen upp.



Bild 3-5: Bottenpanelen med stället i infällt läge



Bild 3-6: Gateway med utfällt ställ

Kapitel 4: Ansluta Wireless-G ADSL-gateway för hemmet

Översikt

Du bör ha fått modemets konfigurationsinformation av installationsteknikern hos Internet-leverantören när bredbandsanslutningen installerades. Annars kan du ringa Internet-leverantören och be om informationen.

När du har den konfigurationsinformation du behöver för din typ av Internet-anslutning kan du börja installera och konfigurera gatewayen.

Om du vill använda en dator med en Ethernet-adapter vid konfiguration av gatewayen, fortsätter du till avsnittet "Kabelanslutning till en dator". Om du vill använda en dator med en trådlös nätverksadapter vid konfiguration av gatewayen fortsätter du till avsnittet "Trådlös anslutning till en dator".

Kabelanslutning till en dator

1. Kontrollera att alla maskinvaror i nätverket är avstängda, inklusive gatewayen och alla datorer.

2. Anslut en telekabel från Line-porten på gatewayens sidopanel till vägguttaget för ADSL-linjen. Om du vill undvika störningar kanske du måste placera en liten enhet som kallas ett mikrofilter (medföljer ej) mellan varje telefon och vägguttaget. Kontakta Internet-leverantören om du har ytterligare frågor.

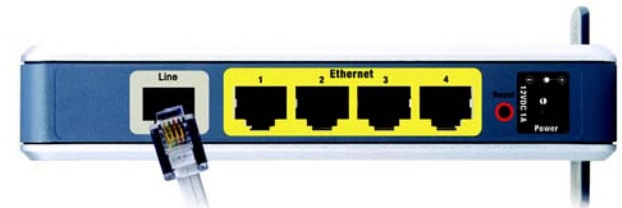


Bild 4-1: Anslut ADSL-linjen



OBS! Om du vill undvika störningar kanske du måste placera en liten enhet som kallas ett mikrofilter (medföljer ej) mellan varje telefon och vägguttaget. Kontakta Internet-leverantören om du har ytterligare frågor.



VIKTIGT! För länder som har teleuttag med RJ-11-anslutningar måste du vara noga med att placera mikrofiltren mellan telefonen och vägguttaget, **inte** mellan gatewayen och vägguttaget, annars fungerar inte ADSL-anslutningen.

För länder som **inte** har teleuttag med RJ-11-anslutningar (t.ex. Frankrike, Sverige, Schweiz, Storbritannien osv.), med undantag för ISDN-användare, måste mikrofiltret användas mellan gatewayen och vägguttaget, eftersom mikrofiltret har RJ-11-anslutning.

Annex B-användare (E1- och DE-versionerna av gatewayen) måste använda den medföljande specialkabeln för anslutning av gatewayen till vägguttaget (RJ-45 till RJ-12). Om behöver en splitter eller specialuttag kontaktar du tjänsteleverantören.

3. Anslut den ena änden av Ethernet-nätverkskabeln till en av Ethernet-portarna (märkt 1-4) på baksidan av gatewayen och den andra änden till en Ethernet-port på en dator.

   Upprepa steget om du vill ansluta fler datorer, en switch eller andra nätverksenheter till gatewayen.

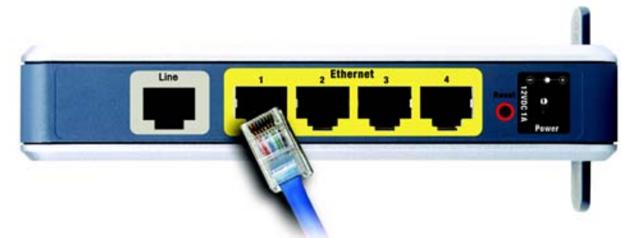


Bild 4-2: Anslut en dator

4. Anslut den medföljande strömadaptern till gatewayens strömport och anslut sedan strömadaptern till ett eluttag.



OBS! Du bör alltid ansluta gatewayens strömadapter i ett förgreningsuttag med strömskydd.

   Strömlysdioden på frontpanelen lyser med grönt sken när strömadaptern är ordentligt ansluten. Strömlysdioden blinkar i några sekunder under tiden som självtestet pågår och övergår sedan till att lysa med fast sken. Om lysdioden blinkar i en minut eller mer, se "Bilaga A: Felsökning".



Bild 4-3: Anslut strömmen

5. Starta en av datorerna som är ansluten till gatewayen.

Gå till "Kapitel 5: Konfigurera Wireless-G ADSL-gateway för hemmet".

Trådlös anslutning till en dator

Om du vill använda en trådlös anslutning för åtkomst till gatewayen gör du så här:

1. Kontrollera att alla maskinvaror i nätverket är avstängda, inklusive gatewayen och alla datorer.
2. Anslut en telekabel från Line-porten på gatewayens bakpanel till vägguttaget för ADSL-linjen. Om du vill undvika störningar kanske du måste placera en liten enhet som kallas ett mikrofilter (medföljer ej) mellan varje telefon och vägguttaget. Kontakta Internet-leverantören om du har ytterligare frågor.



OBS! Om du vill undvika störningar kanske du måste placera en liten enhet som kallas ett mikrofilter (medföljer ej) mellan varje telefon och vägguttaget. Kontakta Internet-leverantören om du har ytterligare frågor.



VIKTIGT! För länder som har teleuttag med RJ-11-anslutningar måste du vara noga med att placera mikrofiltren mellan telefonen och vägguttaget, **inte** mellan gatewayen och vägguttaget, annars fungerar inte ADSL-anslutningen.

För länder som **inte** har teleuttag med RJ-11-anslutningar (t.ex. Frankrike, Sverige, Schweiz, Storbritannien osv.), med undantag för ISDN-användare, måste mikrofiltret användas mellan gatewayen och vägguttaget, eftersom mikrofiltret har RJ-11-anslutning.

Annex B-användare (E1- och DE-versionerna av gatewayen) måste använda den medföljande specialkabeln för anslutning av gatewayen till vägguttaget (RJ-45 till RJ-12). Om behöver en splitter eller specialuttag kontaktar du tjänsteleverantören.

3. Anslut den medföljande strömadaptern till strömporten och anslut sedan strömadaptern till ett eluttag.

   Strömlysdioden på frontpanelen lyser med grönt sken när strömadaptern är ordentligt ansluten. Strömlysdioden blinkar i några sekunder under tiden som självtestet pågår och övergår sedan till att lysa med fast sken. Om lysdioden blinkar i en minut eller mer, se "Bilaga A: Felsökning".

4. Starta en av datorerna i det trådlösa nätverket.
5. Vid första åtkomst till gatewayen genom en trådlös anslutning måste du se till att datorns trådlösa nätverksadaptrar har SSID inställt på **linksys** (gatewayens standardinställning) och att de trådlösa säkerhetsfunktionerna är avaktiverade. När du har anslutit till gatewayen kan du ändra gatewayens och datorns kortinställningar till nätverkets vanliga inställningar.

Gå till "Kapitel 5: Konfigurera Wireless-G ADSL-gateway för hemmet".

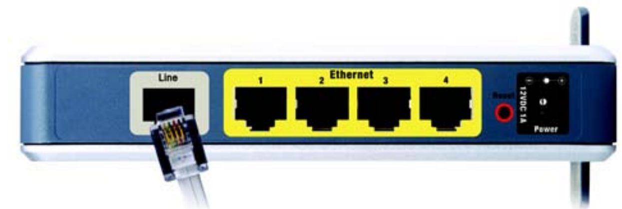


Bild 4-4: Anslut ADSL-linjen



Bild 4-5: Anslut strömmen



OBS! Du bör alltid ändra SSID från standardvärdet **linksys** och aktivera de trådlösa säkerhetsfunktionerna.

Kapitel 5: Konfigurera Wireless-G ADSL-gateway för hemmet

Översikt

Konfigurera gatewayen genom att följa stegen i detta kapitel och använda det webbaserade konfigurationsverktyget. I det här kapitlet beskrivs de olika sidorna i verktyget och de viktigaste funktionerna på sidorna. Verktyget kan nås via en webbläsare på en dator som är ansluten till gatewayen. För en grundläggande nätverkskonfiguration behöver de flesta användare bara använda följande skärmbilder i verktyget:

- Basic Setup (Grundläggande inställningar). På skärmbilden Basic Setup (Grundläggande inställningar) anger du de inställningar du fått av Internet-leverantören.
- Management (Hantering). Klicka på fliken **Administration** och sedan på fliken **Management** (Hantering). Gatewayens standardanvändarnamn och lösenord är admin. För säkerhets skull bör du ange ett nytt lösenord.

Det finns sju huvudflikar: Setup (Konfiguration), Wireless (Trådlöst), Security (Säkerhet), Access Restrictions (Åtkomstbegränsningar), Applications & Gaming (Tillämpningar och spel), Administration och Status. När du klickar på någon av huvudflikarna visas fler flikar.

Setup (Konfiguration)

- Basic Setup (Grundläggande inställningar). På den här skärmbilden anger du inställningar för Internet-anslutningen och nätverket.
- DDNS. Om du vill aktivera gatewayens DDNS-funktion (Dynamic Domain Name System) fyller du i fältet på den här skärmbilden.
- Advanced Routing (Avancerad routing). På den här skärmbilden kan du ändra NAT- och routingkonfigurationer.

Wireless (Trådlöst)

- Basic Wireless Settings (Grundläggande trådlösa inställningar). På den här skärmbilden kan du välja inställningar för det trådlösa nätverket.
- Wireless Security (Trådlös säkerhet) På den här skärmbilden konfigurerar du inställningar för trådlös säkerhet.
- Wireless Access (Trådlös åtkomst). På den här skärmbilden kan du styra åtkomsten till det trådlösa nätverket.
- Advanced Wireless Settings (Avancerade trådlösa inställningar). På den här skärmbilden gör du avancerade inställningar för det trådlösa nätverket.



HAR DU: Har du aktiverat TCP/IP på dina datorer? Datorer kommunicerar över nätverket med hjälp av detta protokoll. Se Windows-hjälpen för mer information om TCP/IP.



OBS! För högre säkerhet bör du ändra lösenordet på fliken Administration.

Security (Säkerhet)

På den här skärmbilden kan du aktivera eller avaktivera brandväggen, konfigurera filter, blockera WAN-begäran och aktivera eller avaktivera VPN-genomströmning (Virtual Private Networks).

***vpn** (virtual private network): en säkerhetsåtgärd som skyddar data när det lämnar ett nätverk och går till ett annat via Internet.*

Access Restrictions (Åtkomstbegränsningar)

- Internet Access (Internet-åtkomst). På den här skärmbilden kan du styra Internet-användningen och -trafiken i det lokala nätverket.

Applications & Gaming (Tillämpningar och spel)

- Single Port Forwarding (Vidarebefordran av en port). På den här skärmbilden kan du konfigurera vanliga tjänster eller tillämpningar som kräver vidarebefordran till en port.
- Port Range Forwarding (Vidarebefordran av portintervall). Om du vill konfigurera offentliga tjänster eller andra specialiserade Internet-tillämpningar som kräver vidarebefordran till ett intervall med portar använder du den här skärmbilden.
- Port Triggering (Portutlösare). Om du vill konfigurera utlösta intervall och vidarebefordrade intervall för Internet-tillämpningar klickar du på den här fliken.
- DMZ. Om du vill tillåta att en lokal dator exponeras för Internet för användning av specialtjänster använder du den här skärmbilden.
- QoS. Använd QoS (Quality of Service) till att tilldela olika prioritetsnivåer till olika typer av dataöverföringar.

Administration

- Management (Hantering). På den här skärmbilden kan du ändra gatewayens åtkomst, SNMP-inställningar (Simple Network Management Protocol), UPnP (Universal Plug and Play), IGMP-Proxy (IGMP står för Internet Group Multicast Protocol) och inställningar för hantering av den trådlösa kommunikationen.
- Reporting (Rapportering). Om du vill visa eller spara aktivitetsloggar klickar du på den här fliken.
- Diagnostics (Diagnostik). På den här skärmbilden kan du köra ett Ping-test.
- Backup&Restore (Säkerhetskopiering och återställning). På den här skärmbilden kan du säkerhetskopiera eller återställa gatewayens konfiguration.
- Factory Defaults (Fabriksinställningar). Om du vill återställa gatewayens fabriksinställningar använder du den här skärmbilden.
- Firmware Upgrade (Uppgradera fast programvara). Klicka på den här fliken om du vill uppgradera gatewayens fasta programvara.
- Reboot (Omstart). Om du behöver göra en hård eller mjuk omstart av gatewayen använder du den här skärmbilden.

Status

- Gateway. Den här skärmbilden innehåller statusinformation om gatewayen.
- Local Network (Lokalt nätverk). Här visas statusinformation om det lokala nätverket.
- Wireless (Trådlöst). Den här skärmbilden innehåller statusinformation om det trådlösa nätverket.
- DSL Connection (DSL-anslutning). Den här skärmbilden innehåller statusinformation om DSL-anslutningen.



Bild 5-1: Inloggningsskärmbilden

Hur du ansluter till det webbaserade verktyget

Du ansluter till det webbaserade verktyget genom att starta Internet Explorer eller Netscape Navigator och sedan ange gatewayens standard-IP-adress, **192.168.1.1**, i *adressfältet*. Tryck sedan på **Enter.**

En inloggningsskärmbild visas (en liknande skärmbild visas för användare av Windows XP). Ange **admin** (standardanvändarnamnet) i fältet *User Name* (Användarnamn) och ange sedan **admin** (standardlösenordet) i fältet *Password* (Lösenord). Klicka på **OK**.

Fliken Setup (Inställningar)

Fliken Basic Setup (Grundläggande inställningar)

Den första skärmbilden som visas är fliken Basic Setup (Grundläggande inställningar). Där kan du ändra de allmänna inställningarna för gatewayen. Ändra inställningarna enligt anvisningarna här och klicka sedan på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

Internet Setup (Internet-inställningar)

- Internet Connection Type (Internet-anslutningstyp). Gatewayen stöder fem inkapslingsmetoder: RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA och Bridged Mode Only. Välj önskad typ i listrutan. Varje *Basic Setup*-skärmbild (Grundläggande inställningar) och de tillgängliga funktionerna skiljer sig åt beroende på vilken typ av inkapsling du väljer.
- VC Settings (VC-inställningar). Här konfigurerar du VC-inställningar (Virtual Circuit).
  - Multiplexing (Multiplex): Välj **LLC** eller **VC**, beroende på Internet-leverantören.
  - QoS Type (QoS-typ): Välj i listrutan: **CBR** (Continuous Bit Rate) om du vill ange fast bandbredd för röst- eller datatrafik, **UBR** (Unspecific Bit Rate) för tillämpningar som inte är tidskänsliga, t.ex. e-post, eller **VBR** (Variable Bite Rate) för mer skurartad trafik och bandbreddsdelning med andra tillämpningar.

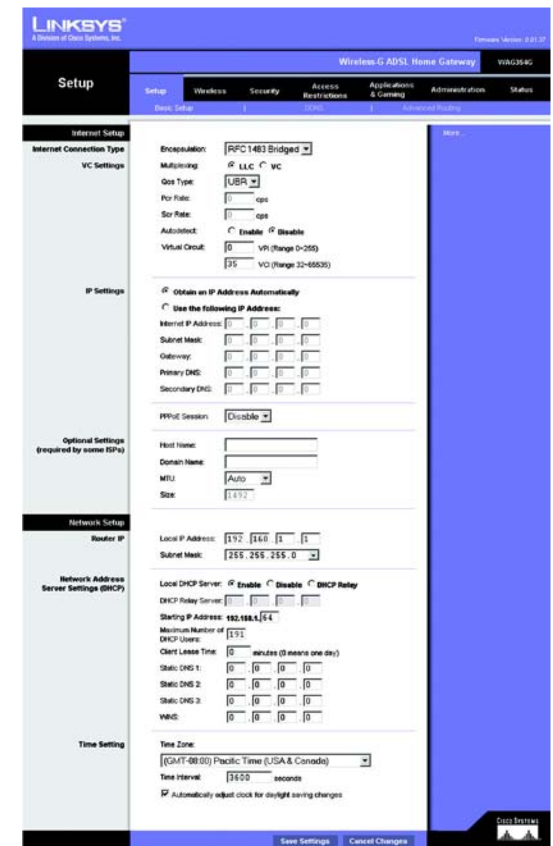


Bild 5-2: Basic Setup (Grundläggande inställningar)

- Pcr Rate (Pcr-hastighet): Du räknar ut Peak Cell Rate genom att dela DSL-linjens hastighet med 424. Då får du den högsta hastighet som avsändaren kan skicka celler med. Ange hastigheten i fältet (om Internet-leverantören kräver det).

- Scr Rate (Scr-hastighet): Värdet Sustain Cell Rate ställer in den genomsnittliga cellhastighet som kan överföras. SCR-värdet är normalt mindre än PCR-värdet. Ange hastigheten i fältet (om din Internet-leverantör kräver det).

- Autodetect (Automatisk avkänning): Välj **Enable** (Aktivera) om du vill att inställningarna ska anges automatiskt eller **Disable** (Avaktivera) om du vill ange värdena manuellt.

- Virtual Circuit (Virtuell krets): Dessa fält består av två objekt: VPI (Virtual Path Identifier) och VCI (Virtual Channel Identifier). Internet-leverantören bistår med korrekta inställningar för dessa fält.

- IP Settings (IP-inställningar). Följ anvisningarna i avsnittet för din typ av inkapsling.

RFC 1483 Bridged (Bryggkopplad)

Dynamisk IP-adress

IP Settings (IP-inställningar). Välj **Obtain an IP Address Automatically** (Hämta en IP-adress automatiskt) om din Internet-leverantör uppger att du ansluter via en dynamisk IP-adress.

Bild 5-3: RFC 1483 Bridged (Bryggkopplad) - Dynamisk IP-adress

Statisk IP-adress

Om du måste använda en permanent (statisk) IP-adress för att ansluta till Internet väljer du **Use the following IP Address** (Använd följande IP-adress).

- Internet IP Address (Internet-IP-adress). Det här är gatewayens IP-adress, när den ses från WAN eller från Internet. Internet-leverantören förser dig med den IP-adress du ska ange här.

- Subnet Mask (Nätmask): Det här är gatewayens nätmask. Internet-leverantören förser dig med nätmasken.

- Gateway: Internet-leverantören förser dig med den standardinställda gateway-adressen, det vill säga IP-adressen till Internet-leverantörens server.

- Primary DNS (Primär DNS) (obligatoriskt) och Secondary DNS (Sekundär DNS) (valfritt). Internet-leverantören förser dig med minst en DNS-adress (Domain Name System).

Bild 5-4: RFC 1483 Bridged (Bryggkopplad) - Statisk IP-adress

RFC 1483 Routed (Dirigerad)

Om du måste använda RFC 1483 Routed (Dirigerad), väljer du **RFC 1483 Routed** (Dirigerad).

- Internet IP Address (Internet-IP-adress). Det här är gatewayens IP-adress, när den ses från WAN eller från Internet. Internet-leverantören förser dig med den IP-adress du ska ange här.
- Subnet Mask (Nätmask): Det här är gatewayens nätmask. Internet-leverantören förser dig med nätmasken.
- Gateway: Internet-leverantören förser dig med den förinställda gateway-adressen, det vill säga IP-adressen till Internet-leverantörens server.
- Primary DNS (Primär DNS) (obligatoriskt) och Secondary DNS (Sekundär DNS) (valfritt). Internet-leverantören förser dig med minst en DNS-serveradress (Domain Name System).

Bild 5-5: RFC 1483 Routed (Dirigerad)

RFC 2516 PPPoE

En del DSL-baserade Internet-leverantörer använder sig av PPPoE (Point-to-Point Protocol over Ethernet) för att upprätta anslutningar till Internet. Om du ansluter till Internet via en DSL-linje måste du kontakta Internet-leverantören och fråga om de använder PPPoE. Om de gör det måste du aktivera PPPoE.

- Service Name (Tjänstenamn). Ange namnet på PPPoE-tjänsten i det här fältet.
- User Name (Användarnamn) och Password (Lösenord). Skriv det användarnamn och lösenord som du fått av Internet-leverantören.
- Connect on Demand: Max Idle Time (Anslut på begäran: Maximal vilotid). Du kan konfigurera gatewayen så att den kopplar ned Internet-anslutningen när den varit inaktiv under en viss tid (Max Idle Time). Om Internet-anslutningen har avbrutits p.g.a inaktivitet ser funktionen Connect on Demand (Anslut på begäran) till att gatewayen automatiskt återupprättar anslutningen så snart du försöker ansluta till Internet igen. Om du vill använda den här funktionen klickar du på alternativknappen **Connect on Demand** (Anslut på begäran). I fältet *Max Idle Time* (Maximal vilotid) anger du efter hur många minuters inaktiv tid du vill att Internet-anslutningen ska brytas.
- Keep Alive: Redial Period (Behåll anslutning: Återuppringningsperiod). Om du väljer det här alternativet kontrollerar gatewayen Internet-anslutningen med jämna mellanrum. Om du är nedkopplad återupprättar gatewayen anslutningen automatiskt. Om du vill använda den här funktionen klickar du på alternativknappen **Keep Alive** (Behåll anslutning). I fältet *Redial Period* (Återuppringningsperiod) anger du hur ofta du vill att gatewayen ska kontrollera Internet-anslutningen. Standardvärdet är **20** sekunder.

Bild 5-6: RFC 2516 PPPoE

RFC 2364 PPPoA

En del DSL-baserade Internet-leverantörer använder sig av PPPoA (Point-to-Point Protocol over ATM) för att upprätta anslutningar till Internet. Om du ansluter till Internet via en DSL-linje måste du kontakta Internet-leverantören och fråga om de använder PPPoA. Om de gör det måste du aktivera PPPoA.

- User Name (Användarnamn) och Password (Lösenord). Skriv det användarnamn och lösenord som du fått av Internet-leverantören.
- Connect on Demand: Max Idle Time (Anslut på begäran: Maximal vilotid). Du kan konfigurera gatewayen så att den kopplar ned Internet-anslutningen när den varit inaktiv under en viss tid (Max Idle Time). Om Internet-anslutningen har avbrutits p.g.a inaktivitet, ser funktionen Connect on Demand (Anslut på begäran) till att gatewayen automatiskt återupprättar anslutningen så snart du försöker ansluta till Internet igen. Om du vill använda den här funktionen klickar du på alternativknappen **Connect on Demand** (Anslut på begäran). I fältet *Max Idle Time* (Maximal vilotid) anger du efter hur många minuters inaktiv tid du vill att Internet-anslutningen ska brytas.
- Keep Alive: Redial Period (Behåll anslutning: Återuppringningsperiod). Om du väljer det här alternativet kontrollerar gatewayen Internet-anslutningen med jämna mellanrum. Om du är nedkopplad återupprättar gatewayen anslutningen automatiskt. Om du vill använda den här funktionen klickar du på alternativknappen **Keep Alive** (Behåll anslutning). I fältet *Redial Period* (Återuppringningsperiod) anger du hur ofta du vill att gatewayen ska kontrollera Internet-anslutningen. Standardvärdet är **20** sekunder.

Internet Setup
Internet Connection Type
VC Settings
Encapsulation: RFC 2364 PPPoA
Multiplexing: LLC VC
Qos Type: UBR
Pcr Rate: 0 cps
Scr Rate: 0 cps
Autodetect: Enable Disable
Virtual Circuit: 0 VPI (Range 0~255)
35 VCI (Range 32~65535)
PPPoA Settings
User Name:
Password:
Connect on Demand: Max Idle Time 20 Min.
Keep Alive: Redial Period 20 Sec.

Bild 5-7: RFC 2364 PPPoA

Bridged Mode Only (Endast bryggkopplat läge)

Om du använder gatewayen som brygga, vilket får gatewayen att fungera som ett fristående modem väljer du **Bridged Mode Only** (Endast bryggkopplat läge). Alla NAT- och routinginställningar avaktiveras i detta läge.

Internet Setup
Internet Connection Type
VC Settings
Encapsulation: Bridge Mode Only
Multiplexing: LLC VC
Qos Type: UBR
Pcr Rate: 0 cps
Scr Rate: 0 cps
Autodetect: Enable Disable
Virtual Circuit: 0 VPI (Range 0~255)
35 VCI (Range 32~65535)
Optional Settings (required by some ISPs)
Host Name:
Domain Name:
MTU: Auto
Size: 1492

Bild 5-8: Bridged Mode Only (Endast bryggkopplat läge)

Optional Settings (Valfria inställningar) (krävs av vissa Internet-leverantörer)

- Host Name (Värdnamn) och Domain Name (Domännamn). I de här fälten kan du ange ett värd- och ett domännamn för gatewayen. Vissa Internet-leverantörer kräver de här namnen som identifikation. Du kanske måste fråga Internet-leverantören om din bredbandsanslutning till Internet har konfigurerats med ett värd- respektive domännamn. I de flesta fall kan du lämna dessa fält tomma.
- MTU och Size (Storlek). Med inställningen MTU (Maximum Transmission Unit) anger du den största tillåtna paketstorleken för nätverksöverföring. Välj **Manual** (Manuell) och ange sedan önskat värde i fältet *Size* (Storlek). Det rekommenderas att du anger ett värde mellan 1200 och 1500. Som standard konfigureras MTU automatiskt.

Network Setup (Nätverksinställningar)

- Router IP (Router-IP). Här visas värdena för gatewayens lokala IP-adress och nätmask. I de flesta fall går det bra att behålla standardinställningarna.

- Local IP Address (Lokal IP-adress): Standardvärdet är **192.168.1.1**.
- Subnet Mask (Nätmask): Standardvärdet är **255.255.255.0**.

- Network Address Server Settings (DHCP) (Inställningar för nätverksadresserver (DHCP)). Här konfigurerar du gatewayens DHCP-inställningar (Dynamic Host Configuration Protocol).
  - Local DHCP Server (Lokal DHCP-server). En DHCP-server (Dynamic Host Configuration Protocol) tilldelar automatiskt en IP-adress till varje dator i nätverket. Såvida du inte redan har en DHCP-server rekommenderar vi att du låter gatewayen vara aktiverad som en sådan. Du kan också använda gatewayen i DHCP-reläläge.
  - DHCP Relay Server (DHCP-reläserver). Om du aktiverar DHCP Relay mode (DHCP-reläläge) för inställningen *Local DHCP Server* (Lokal DHCP-server), anger du DHCP-serverns IP-adress i fälten.
  - Starting IP Address (Start-IP-adress). Ange ett värde som DHCP-servern ska börja på vid tilldelning av IP-adresser. Detta värde måste vara 192.168.1. 2 eller högre, eftersom standard-IP-adressen för gatewayen är 192.168.1.1.
  - Maximum Number of DHCP Users (Maximalt antal DHCP-användare). Ange det maximala antalet användare/klienter som kan erhålla en IP-adress. Antalet varierar beroende på den start-IP-adress som angetts.
  - Client Lease Time (Klientlånetid). Det här är den tid som en dator tillåts vara ansluten till gatewayen med den aktuella dynamiska IP-adressen. Ange tiden i minuter som datorn får "låna" den här dynamiska IP-adressen.
  - Statisk DNS 1-3. DNS (Domain Name System) är den metod som Internet använder sig av för att översätta domän- och webbplatsnamn till Internet-adresser eller URL-adresser. Internet-leverantören förser dig med minst en DNS-serveradress. Du kan ange upp till tre DNS-serveradresser här. Gatewayen använder dessa för snabbare åtkomst till fungerande DNS-servrar.
  - WINS. WINS (Windows Internet Naming Service) omvandlar NetBIOS-namn till IP-adresser. Om du använder en WINS-server anger du den serverns IP-adress här. I annat fall lämnar du fältet tomt.
  - Time Setting (Tidsinställning). Välj önskad tidszon för den plats gatewayen står på. Om du vill kan du markera kryssrutan **Automatically adjust clock for daylight saving changes** (Använd sommartid automatiskt).

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.

Bild 5-9: Optional Settings (Valfria inställningar)

Fliken DDNS

Gatewayen har en DDNS-funktion (Dynamic Domain Name System). Med DDNS kan du tilldela ett fast värd- och domännamn till en dynamisk Internet IP-adress. Den är användbar när du har en egen webbplats, FTP-server eller en annan server bakom gatewayen.

Innan du kan använda den här funktionen måste du anmäla dig hos en DDNS-tjänst, t.ex. DynDNS.org eller TZO.com.



Bild 5-10: DynDNS.org

DDNS

DDNS Service (DDNS-tjänst). Om din DDNS-tjänst tillhandahålls av DynDNS.org väljer du **DynDNS.org** i listrutan. Om din DDNS-tjänst tillhandahålls av TZO.com väljer du **TZO.com** i listrutan. Om du vill avaktivera DDNS-tjänsten väljer du **Disabled** (Avaktiverad).

DynDNS.org

- User Name (Användarnamn), Password (Lösenord) och Host Name (Värdnamn). Ange användarnamnet, lösenordet och värdnamnet för det konto som du konfigurerar med DynDNS.org.
- Internet IP Address (Internet-IP-adress). Här visas gatewayens aktuella Internet IP-adress. Eftersom den är dynamisk kommer den att ändras.
- Status. Här visas status för anslutningen till DDNS-tjänsten.

TZO.com

- E-mail Address (E-postadress), Password (Lösenord) och Domain Name (Domännamn). Ange e-postadressen, lösenordet och domännamnet för det konto som du konfigurerar med TZO.
- Internet IP Address (Internet-IP-adress). Här visas gatewayens aktuella Internet IP-adress. Eftersom den är dynamisk kommer den att ändras.
- Status. Här visas status för anslutningen till DDNS-tjänsten.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.



Bild 5-11: TZO.com

Fliken Advanced Routing (Avancerad routing)

På skärmbilden *Advanced Routing* (Avancerad routing) kan du göra inställningar för NAT, dynamisk routing och statisk routing.

Advanced Routing (Avancerad routing)

- Operating Mode (Driftsläge). Här konfigurerar du gatewayens allmänna routinginställningar.
  - NAT. NAT är en säkerhetsfunktion som är aktiverad som standard. Den gör det möjligt för gatewayen att översätta IP-adresser i det lokala nätverket till en annan IP-adress för Internet. Om du vill avaktivera NAT klickar du på alternativknappen **Disabled** (Avaktiverad).
  - RIP. Om du har flera routrar kan du använda RIP (Routing Information Protocol) så att routrarna kan utbyta routinginformation med varandra. Om du vill använda RIP markerar du alternativknappen **Enabled** (Aktiverad). I annat fall behåller du standardvärdet **Disabled** (Avaktiverad).
  - Send Default Route (Sänd standardrouting). Om du vill använda RIP version 1 för routing markerar du alternativknappen **Enabled** (Aktiverad). I annat fall behåller du standardvärdet **Disabled** (Avaktiverad).
  - Interface (Gränssnitt). Den här inställningen är tillgänglig när du har konfigurerat en statisk routing och vill välja ett gränssnitt för den. Välj det gränssnitt som gatewayen ska använda: **LAN/Wireless** (LAN/Trådlöst) eller **Internet**.
- Dynamic Routing (Dynamisk routing). Med den här funktionen kan du ange att gatewayen automatiskt ska justeras för fysiska ändringar i nätverkets layout. Med RIP fastställer gatewayen nätverkspaketens väg utifrån de lägsta antalet hopp mellan källan och destinationen. RIP-protokollet sänder regelbundet ut routinginformation till andra gatewayer i nätverket.
  - Transmit RIP Version (Överför RIP-version). Om du vill överföra RIP-meddelanden väljer du önskat protokoll: **RIP1, RIP1-Compatible (RIP-1-kompatibelt) eller RIP2**. Om du inte vill överföra RIP-meddelanden väljer du **None** (Inget).
  - Receive RIP Version (Ta emot RIP-version). Om du vill ta emot RIP-meddelanden väljer du önskat protokoll: **RIP1** eller **RIP2.** Om du inte vill överföra RIP-meddelanden väljer du **None** (Inget).
  - Multicast eller Broadcast. Du kan skicka RIP med endera metoden. Om du vill använda multicasting väljer du **Multicast**. Om du vill använda Broadcast väljer du **Broadcast**.
- Static Routing (Statisk routing). Om gatewayen är ansluten till mer än ett nätverk kan det bli nödvändigt att konfigurera en statisk routing mellan dem. En statisk routing är en förbestämd väg som nätverksinformation måste färdas för att nå en viss värd eller ett visst nätverk. Om du vill skapa en statisk routing ändrar du följande inställningar:

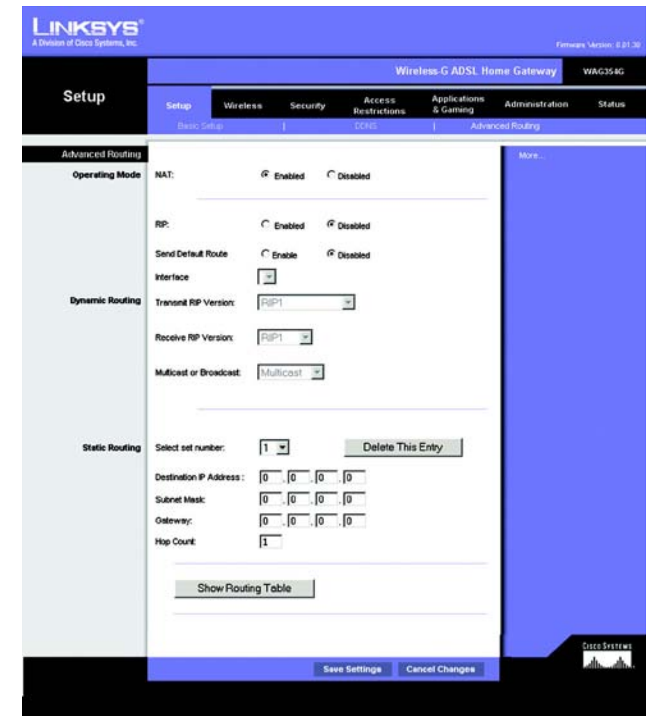


Bild 5-12: Advanced Routing (Avancerad routing)

- Välj uppsättningsnummer. Välj numret för den statiska routingen i listrutan. Gatewayen hanterar upp till 20 statiska routingposter. Om du vill ta bort en routing markerar du posten och klickar sedan på **Delete This Entry** (Ta bort den här posten).
- Destination IP Address (Destinations-IP-adress). Destinations-IP-adressen är adressen till fjärrnätverket eller värden som du vill tilldela en statisk routing till. Ange IP-adressen till den värd som du vill skapa en statisk routing till. Om du bygger en routing till ett helt nätverk måste du se till att nätverksdelen av IP-adressen är inställd på 0.
- Subnet Mask (Nätmask): Ange nätmasken som avgör vilken del av en IP-adress som är nätverksdelen, och vilken del som är värddelen.
- Gateway: Ange IP-adressen för den gatewayenhet som medger kontakt mellan gatewayen och fjärrnätverket eller värden.
- Hop Count (Antal hopp). Det här är antalet hopp till varje nod fram tills dess destinationen nås (högst 16 hopp). Ange antalet hopp i motsvarande fält.

- Show Routing Table (Visa routingtabell). Klicka på knappen **Show Routing Table** (Visa routingtabell) om du vill öppna en skärmbild som visar hur data leds genom ditt lokala nätverk. För varje väg visas destination-LAN:ets IP-adress, nätmask, gateway och gränssnitt. Klicka på knappen **Refresh** (Uppdatera) om du vill uppdatera informationen. Klicka på **Close** (Stäng) om du vill gå tillbaka till föregående skärmbild.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.

Routing Table Entry List Refresh

Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	LAN & Wireless

Close

Bild 5-13: Routing Table (Routingtabell)

Fliken Wireless (Trådlöst)

Fliken Basic Wireless Settings (Grundläggande trådlösa inställningar)

På den här skärmbilden kan du välja läge för det trådlösa nätverket och trådlös säkerhet.

Wireless Network (Trådlöst nätverk)

- Trådlöst nätverksläge: Om du har 802.11g- och 802-11b-enheter i nätverket behåller du standardinställningen **Mixed** (Blandat). Om du bara har 802.11g-enheter väljer du **802.11g**. Om du bara har 802.11b-enheter väljer du **802.11b**. Om du vill avaktivera det trådlösa nätverket väljer du **Disabled** (Avaktiverad).
- Wireless Network Name (SSID) (Trådlöst nätverksnamn). Ange namnet för det trådlösa nätverket i fältet. SSID:t (Service Set Identifier) är det nätverksnamn som delas av alla enheter i det trådlösa nätverket. Det måste vara identiskt för alla enheter i det trådlösa nätverket. Namnet är skiftlägeskänsligt och får inte överstiga 32 alfanumeriska tecken (alla tangentbordstecken kan användas). Av säkerhetsskäl rekommenderas du att ändra det standardinställda SSID-värdet (linksys) till ett unikt värde.
- Wireless Channel (Trådlös kanal). I listan väljer du en lämplig kanal som motsvarar dina nätverksinställningar. Alla enheter i det trådlösa nätverket måste använda samma kanal om de ska fungera korrekt. Trådlösa datorer och klienter känner automatiskt av gatewayens trådlösa kanal.
- Wireless SSID Broadcast (Trådlös SSID Broadcast). När trådlösa datorer eller klienter söker i det lokala nätet efter trådlösa nätverk att koppla till kommer gatewayen att känna av SSID Broadcast. Om du vill sända gatewayens SSID behåller du standardinställningen **Enable** (Aktivera). Om du inte vill sända gatewayens SSID väljer du **Disable** (Avaktivera).

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.

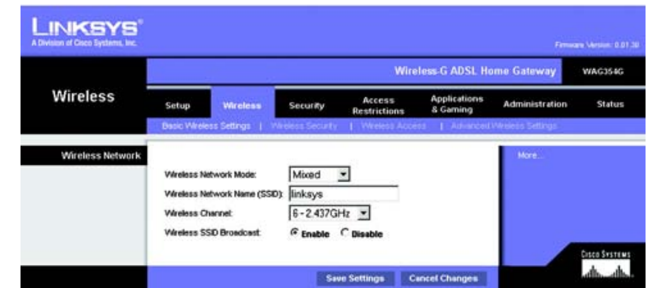


Bild 5-14: Basic Wireless Settings (Grundläggande trådlösa inställningar)

Fliken Wireless Security (Trådlös säkerhet)

Med de här inställningarna konfigurerar du det trådlösa nätverkets säkerhet. Gatewayen stöder två alternativ för trådlös säkerhet: WPA Pre-Shared Key (WPA med för-delad nyckel) och WEP. (WPA står för Wi-Fi Protected Access, som är en säkerhetsstandard som är mer kraftfull än WEP-kryptering. WEP står för Wired Equivalent Privacy.) Dessa behandlas kortfattat här. Mer information om hur du konfigurerar trådlös säkerhet för gatewayen finns i "Bilaga B: Trådlös säkerhet". Om du vill avaktivera de trådlösa säkerhetsfunktionerna väljer du **Disable** (Avaktivera) i listrutan för säkerhetsläge.

WPA Pre-Shared Key (WPA med för-delad nyckel). Ange en WPA-delad nyckel med 8–32 tecken. Slutligen anger du en gruppnyckelförnyelseperiod, vilket anger hur ofta krypteringsnycklarna ska ändras för gatewayen.



Bild 5-15: (WPA med för-delad nyckel)

WEP. WEP är en enkel krypteringsmetod som inte är lika säker som WPA. Om du vill använda WEP väljer du en standardnyckel (detta anger vilken nyckel som ska användas) och en nivå för WEP-krypteringen, **64 bitar 10 hex-siffror eller 128 bitar 26 hex-siffror.** Sedan genererar du en WEP-nyckel med ett lösenord eller anger WEP-nyckeln manuellt.

- WEP-kryptering WEP är en förkortning av Wired Equivalent Privacy och är en krypteringsmetod som används för att skydda din trådlösa datakommunikation. WEP använder 64-bitars eller 128-bitars nycklar för åtkomstkontroll av nätverket och säkerhet för alla dataöverföringar. För att kunna koda av dataöverföringar måste alla enheter i nätverket ha samma WEP-nyckel. Högre krypteringsnivåer ger bättre säkerhet, men p.g.a komplexiteten hos krypteringen kan de minska nätverksprestandan. Om du vill aktivera WEP väljer du **64 bits 10 hex digits** (64-bitars 10 hexsiffror) eller **128 bits 26 hex digits** (128-bitars 26 hexsiffror).

- Default Transmit Key (Standardöverföringsnyckel) Välj vilken WEP-nyckel (1-4) som ska användas när gatewayen skickar data. Se till att den mottagande enheten (trådlös dator eller klient) använder samma nyckel.

- Passphrase (Lösenordsfras). Istället för att ange WEP-nycklar manuellt kan du ange en lösenordsfras. Lösenordsfrasen används till att generera en eller flera WEP-nycklar. Lösenordsfrasen är skiftlägeskänslig och får inte överstiga 32 alfanumeriska tecken. (Lösenordsfrasfunktionen är kompatibel med Linksys trådlösa produkter och kan inte användas med Windows XPs nollkonfiguration. Om du vill kommunicera med trådlösa produkter från andra tillverkare eller Windows XPs nollkonfiguration, måste du anteckna den WEP-nyckel som genereras i fältet *Key 1* (Nyckel 1) och sedan ange den manuellt i den trådlösa datorn eller klienten.) När du har angett lösenordet klickar du på knappen **Generate** (Generera) så skapas WEP-nycklar.

- WEP Nycklar 1-4. Med WEP-nycklar kan du skapa ett krypteringsschema för trådlösa nätverksöverföringar. Om du inte använder någon lösenordsfras måste du ange en uppsättnings värden manuellt. (Lämna inte ett nyckelfält tomt och ange inte alla nollor - de är inte giltiga nyckelvärden.) Om du använder 64-bitars WEP-kryptering måste nyckeln bestå av exakt 10 hexadecimala tecken. Om du använder 128-bitars WEP-kryptering måste nyckeln bestå av exakt 26 hexadecimala tecken. Giltiga hexadecimala tecken är "0" till "9" och "A" till "F".

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna. Mer information om hur du konfigurerar trådlös säkerhet för gatewayen finns i "Bilaga B: Trådlös säkerhet."



Bild 5-16: WEP

Fliken Wireless Access (Trådlös åtkomst)

Wireless Network Access (Trådlös nätverksåtkomst)

Wireless Network Access (Trådlös nätverksåtkomst). Välj **Allow All** (Tillåt alla) om du vill att alla datorer ska ha åtkomst till det trådlösa nätverket. Om du vill begränsa åtkomst till nätverket väljer du **Restrict Access** (Begränsa åtkomst) och sedan **Prevent** (Förhindra) för att blockera åtkomst för de angivna datorerna eller **Permit only** (Tillåt endast) för att tillåta åtkomst för de angivna datorerna. Klicka på knappen **Edit MAC Address Access List** (Redigera åtkomstlistan för MAC-adresser) så visas skärmbilden *Mac Address Filter List* (MAC-adressfilterlista).

Ange MAC-adresserna för de datorer du vill ange. Om du vill visa en lista med MAC-adresser för trådlösa datorer eller klienter klickar du på knappen **Wireless Client MAC List** (Lista med trådlösa klienters MAC-adresser).

På skärmbilden *Wireless Client MAC List* (Lista med trådlösa klienters MAC-adresser) visas datorer, deras IP-adresser och MAC-adresser. Klicka på knappen Refresh (Uppdatera) om du vill få den senaste informationen. Markera kryssrutan **Enable MAC Filter** (Aktivera MAC-filter) om du vill lägga till en viss dator i MAC-adressfilterlistan, markera kryssrutan **Enable MAC Filter** (Aktivera MAC-filter) och klicka sedan på knappen **Update Filter List** (Uppdatera filterlista). Klicka på knappen **Close** (Stäng) för att återgå till skärmbilden *Wireless Client MAC List* (Lista med trådlösa klienters MAC-adresser).

På skärmbilden *Wireless Client MAC List* (Lista med trådlösa klienters MAC-adresser) klickar du på knappen **Save Settings** (Spara inställningar) om du vill spara denna lista eller på knappen **Cancel Changes** (Avbryt ändringar) om du vill ta bort posterna.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.



Bild 5-17: Wireless Network Access (Trådlös nätverksåtkomst)

MAC Address Filter List

Enter MAC Address Format: xxxxxxxxxxxx/xx:xx:xx:xx:xx:xx

MAC 01: MAC 02: MAC 03: MAC 04: MAC 05: MAC 06: MAC 07: MAC 08: MAC 09: MAC 10:

MAC 11: MAC 12: MAC 13: MAC 14: MAC 15: MAC 16: MAC 17: MAC 18: MAC 19: MAC 20:

Wireless Client MAC List

Save Settings Cancel Changes

Bild 5-18: MAC Address Filter List (MAC-adressfilterlista)



Bild 5-19: Wireless Client MAC List (Lista med trådlösa klienters MAC-adresser)

Fliken Advanced Wireless Settings (Avancerade trådlösa inställningar)

Advanced Wireless (Avancerat trådlöst)

Den här skärmbilden innehåller avancerade trådlösa funktioner för autentiseringstyp, Control TX-hastighet, Signalintervall, DTIM-intervall, fragmenteringsgränsvärde och RTS-gränsvärde.

- Authentication Type (Autentiseringstyp). Standardvärdet är **Auto**, vilket innebär att autentisering av typen Open System (Öppet system) eller Shared Key (Delad nyckel) används. Med autentisering av typen Open System (Öppet system) använder inte sändaren eller mottagaren någon WEP-nyckel för autentisering, men de kan använda WEP för datakryptering. Om du bara vill tillåta autentisering med Open System (Öppet system) väljer du **Open System.** Med autentisering av typen Shared Key (Delad nyckel) använder sändaren och mottagaren en WEP-nyckel för både autentisering och datakryptering. Om du bara vill tillåta autentisering med Shared Key (Delad nyckel) väljer du **Shared Key.** Det rekommenderas att detta alternativ lämnas i standardläget (Auto), eftersom vissa klienter inte kan konfigureras för Shared Key (Delad nyckel).
- Control Tx Rates (Control Tx-hastigheter). Standardhastigheten är **Auto**. Hastigheten bör ställas in utifrån hastigheten i det trådlösa nätverket. Välj mellan olika överföringshastigheter eller behåll standardinställningen **Auto** om du vill låta gatewayen automatiskt använda den snabbast tillgängliga datahastigheten och aktivera funktionen Auto-Fallback (Automatisk tillbakagång). Funktionen Auto-Fallback (Automatisk tillbakagång) förhandlar fram den bästa möjliga anslutningshastigheten mellan gatewayen och en trådlös klient.
- Beacon Interval (Signalintervall). Standardvärdet är **100.** Det här värdet anger frekvensintervallet för signalen. En signal är ett paket som sänds av gatewayen för att synkronisera det trådlösa nätverket.
- DTIM Interval (DTIM-intervall). Standardvärdet är **1.** Det här värdet anger intervallet för DTIM-meddelandet (Delivery Traffic Indication Message). Ett DTIM-fält är en nedräkningsfält som meddelar klienter om nästa fönster för lyssning av broadcast- och multicast-meddelanden. När gatewayen har buffrat broadcast- eller multicast-meddelanden för associerade klienter sänder den nästa DTIM med ett DTIM-intervallvärde. Klienterna hör signalpaketen och vaknar till för att ta emot broadcast- och multicast-meddelandena.
- Fragmentation Threshold (Fragmenteringsgränsvärde). Det här värdet ska lämnas på standardinställningen **2346.** Det anger den maximala storleken för ett paket innan data fragmenteras till flera paket. Om du får en hög paketfelfrekvens kan du minska detta värde något. Om du anger ett för lågt värde kan nätverksprestandan försämras. Det rekommenderas att du bara gör mindre ändringar av detta värde.
- RTS Threshold (RTS-gränsvärde). Det här värdet ska lämnas på standardinställningen **2347**. Om du får problem med inkonsekventa dataflöden, rekommenderas endast mindre ändringar. Om ett nätverkspaket är mindre än den förinställda RTS-gränsvärdesstorleken, aktiveras inte RTS/CTS-mekanismen. Gatewayen skickar RTS-ramar (Request to Send) till en viss mottagande station och förhandlar sedan om sändningen av en dataram. Efter att ha tagit emot en RTS svarar den trådlösa stationen med en CTS-ram (Clear to Send) som bekräftar rätten att påbörja sändningen.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.



Bild 5-20: Advanced Wireless Settings (Avancerade trådlösa inställningar)

Fliken Security (Säkerhet)

På den här skärmbilden visas inställningar för VPN-genomströmning, brandvägg och filter. Med de här funktionerna kan du förbättra nätverkets säkerhet.

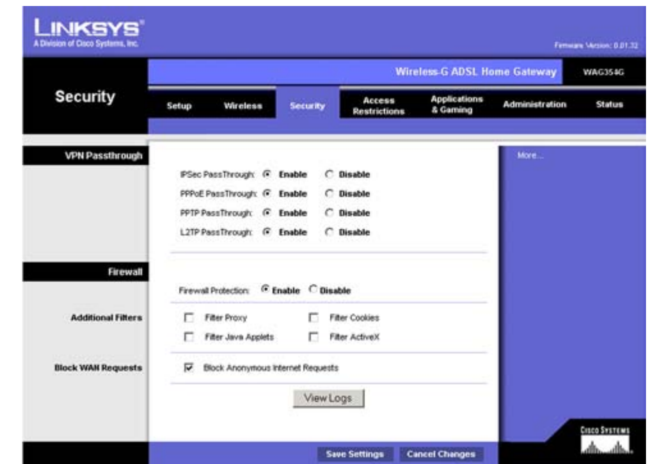


Bild 5-21: Security (Säkerhet)

VPN Passthrough (VPN-genomströmning)

VPN (Virtual Private Networking) är en säkerhetsåtgärd som skapar en säker anslutning mellan två fjärrplatser. Konfigurera dessa inställningar så att gatewayen tillåter att VPN-tunnlar släpps igenom.

- IPSec Passthrough (IPSec-genomströmning) IPSec (Internet Protocol Security) är en svit med protokoll som används för att implementera säkert utbyte av paket på IP-lagret. Om du vill tillåta IPSec Passthrough (IPSec-genomströmning) klickar du på knappen **Enable** (Aktivera). Om du vill avaktivera IPSec Passthrough klickar du på knappen **Disable** (Avaktivera).
- PPPoE Passthrough (PPPoE-genomströmning) Med PPPoE Passthrough (PPPoE-genomströmning) tillåter du att dina datorer använder den PPPoE-klientprogramvara som du fått av Internet-leverantören. Vissa Internet-leverantörer kan begära att du använder denna funktion på gatewayen. Om du vill tillåta PPPoE Passthrough (PPPoE-genomströmning) klickar du på knappen **Enable** (Aktivera). Om du vill avaktivera PPPoE Passthrough klickar du på knappen **Disable** (Avaktivera).
- PPTP Passthrough (PPTP-genomströmning) Det här är den metod som används för att aktivera VPN-sessioner till en Windows NT 4.0- eller 2000-server. Om du vill tillåta PPTP Passthrough (PPTP-genomströmning) klickar du på knappen **Enable** (Aktivera). Om du vill avaktivera PPTP Passthrough klickar du på knappen **Disable** (Avaktivera).
- L2TP Passthrough (L2TP-genomströmning) Det här är en utökning av PPTP-protokollet som används för att aktivera användningen av ett VPN över Internet. Om du vill tillåta L2TP Passthrough klickar du på knappen **Enable** (Aktivera). Om du vill avaktivera L2TP Passthrough klickar du på knappen **Disable** (Avaktivera).

Firewall (Brandvägg)

Du kan aktivera eller avaktivera brandväggen, välja filter som blockerar vissa Internet-datatyper och blockera anonyma Internet-begäran.

Om du vill använda brandväggen klickar du på **Enable** (Aktivera). Om du inte vill använda brandväggen klickar du på **Disable** (Avaktivera).

Ytterligare filter

- Filter Proxy (Filter-proxy). Om du väljer att använda WAN-proxyservrar kan det äventyra gatewayens säkerhet. Om du inte använder funktionen får du inte åtkomst till några WAN-proxyservrar. Om du vill använda proxyfiltrering markerar du kryssrutan.
- Filter Cookies (Filtrera cookies). En cookie är data som sparas på datorn och som används av webbplatser när du interagerar med dem. Om du vill använda cookiefiltrering markerar du kryssrutan.

- Filter Java Applets (Filtrera Java-appletprogram). Java är ett programmeringsspråk för webbplatser. Om du avvisar Java-appletprogram riskerar du att inte få tillgång till webbplatser som använder detta programmeringsspråk. Om du vill använda filtrering av Java-appletprogram markerar du kryssrutan.
- Filter ActiveX (Filtrera ActiveX). ActiveX är ett programmeringsspråk för webbplatser. Om du avvisar ActiveX riskerar du att inte få tillgång till webbplatser som använder detta programmeringsspråk. Om du vill använda ActiveX-filtrering markerar du kryssrutan.

Block WAN Requests (Blockera WAN-begäran)

- Block Anonymous Internet Requests (Blockera anonyma Internet-begäran). Med den här funktionen förhindrar du att nätverket "pingas" eller upptäcks och förstärker nätverkets säkerhet genom att dölja nätverksportarna så att det blir svårare för inkräktare att upptäcka nätverket. Välj **Block Anonymous Internet Requests** (Blockera anonyma Internet-begäran) om du vill blockera anonyma Internet-begäran eller avmarkera alternativet och tillåta dem.

Om du vill visa aktivitetsloggar för dina säkerhetsåtgärder klickar du på knappen **View Logs** (Visa loggar). Klicka på knappen **Clear** (Rensa) om du vill rensa logginformationen. Klicka på knappen **pageRefresh** (Uppdatera sida) om du vill uppdatera informationen. Klicka på knappen **Previous Page** (Föregående sida) om du vill gå till den föregående sidan med information. Klicka på knappen **Next Page** (Nästa sida) om du vill gå till nästa sida med information.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.

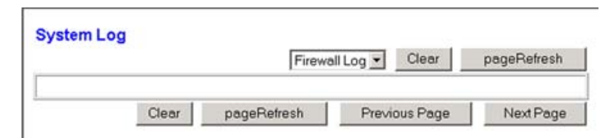


Bild 5-22: Firewall Log (Brandväggslogg)

Fliken Access Restrictions (Åtkomstbegränsningar)

Fliken Internet Access (Internet-åtkomst)

På skärmbilden *Internet Access* (Internet-åtkomst) kan du blockera eller tillåta vissa typer av Internet-användning. Du kan ange regler för Internet-åtkomst för vissa datorer och blockera webbplatser efter URL-adresser eller nyckelord.

Internet Access Policy (Regler för Internet-åtkomst). Åtkomsten kan hanteras av regler. Med inställningarna på den här skärmbilden kan du upprätta åtkomstregler (när du har klickat på knappen **Save Settings** (Spara inställningar)). Om du väljer en regel i listrutan visas inställningarna för den regeln. Om du vill ta bort en regel markerar du regelns nummer och klickar sedan på knappen **Delete** (Ta bort). Om du vill visa alla regler klickar du på knappen **Summary** (Sammanfattning). (Du kan ta bort regler från skärmbilden *Summary* (Sammanfattning) genom att markera regeln eller reglerna och sedan klicka på knappen **Delete** (Ta bort). Om du vill återgå till skärmbilden Internet Access (Internet-åtkomst) klickar du på knappen **Close** (Stäng).)

Status. Som standard är reglerna avaktiverade. Om du vill aktivera en regel markerar du regelns nummer i listrutan och klickar sedan på alternativknappen bredvid *Enable* (Aktivera).

Så här skapar du en regel för Internet-åtkomst:

1. Markera ett nummer i listrutan *Access Policy* (Åtkomstregel).
2. Om du vill aktivera den här regeln klickar du på alternativknappen bredvid *Enable*. (Aktivera)
3. Ange ett regelnamn i motsvarande fält.

Bild 5-23: Internet Access (Internet-åtkomst)

Bild 5-24: Internet Policy Summary (Sammanfattning av Internet-regel)

4. Klicka på knappen **Edit List of PCs** (Redigera lista med datorer) om du vill välja de datorer som ska påverkas av regeln. Skärmbilden *List of PCs* (Lista med datorer) visas. Du kan välja en dator efter MAC-adress eller IP-adress. Du kan också ange ett intervall med IP-adresser om du vill att regeln ska påverka en grupp med datorer. När du har gjort ändringarna klickar du på knappen **Save Settings** (Spara inställningar) eller **Cancel Changes** (Avbryt inställningar) om du vill avbryta utan att spara ändringarna.

5. Klicka på önskat alternativ, **Deny** (Avvisa) eller **Allow** (Tillåt) beroende på om du vill blockera eller tillåta Internet-åtkomst för de datorer du angett på skärmbilden *List of PCs* (Lista med datorer).

6. Bestäm vilka dagar och vilka tider som du vill att denna regel ska gälla. Välj de enskilda dagar som regeln ska gälla, eller välj **Everyday** (Varje dag). Ange sedan ett tidsintervall i timmar och minuter under vilken regeln ska gälla, eller välj **24 Hours** (24 timmar).

7. Om du vill blockera webbplatser med vissa URL-adresser, anger du varje URL i ett separat fält bredvid *Website Blocking by URL Address* (Webbplatsblockering efter URL-adress).

8. Om du vill blockera webbplatser med vissa nyckelord anger du varje nyckelord i ett separat fält bredvid *Website Blocking by Keyword* (Webbplatsblockering efter nyckelord).

9. Du kan filtrera åtkomst till olika tjänster på Internet, t.ex. FTP eller telnet, genom att välja tjänster i listrutorna bredvid *Blocked Services* (Blockerade tjänster).

   Ange sedan det portintervall som du vill filtrera.

   Om den tjänst som du vill blockera inte finns med i listan eller om du vill redigera inställningarna för en tjänst klickar du på knappen **Add/Edit Service** (Lägg till/redigera tjänst). Skärmbilden *Port Services* (Porttjänster) visas.

   Om du vill lägga till en tjänst anger du tjänstens namn i fältet *Service Name* (Tjänstenamn). Välj protokollet i listrutan *Protocol* (Protokoll) och ange sedan intervallet i fälten *Port Range* (Portintervall). Klicka sedan på knappen **Add** (Lägg till).

   Om du vill ändra en tjänst markerar du den i listan till höger. Ändra namnet, protokollinställningarna eller portintervallet. Klicka sedan på knappen **Modify** (Ändra).

   Om du vill ta bort en tjänst markerar du den i listan till höger. Klicka sedan på knappen **Delete** (Ta bort).

   När du är klar med skärmbilden *Port Services* (Porttjänster) klickar du på knappen **Apply** (Använd) för att spara ändringarna. Om du vill avbryta ändringarna klickar du på knappen **Cancel** (Avbryt). Om du vill stänga skärmbilden *Port Services* (Porttjänster) och återgå till skärmbilden *Access Restrictions* (Åtkomstbegränsningar) klickar du på knappen **Close** (Stäng).

10. Spara regelns inställningar genom att klicka på **Save Settings** (Spara inställningar). Om du vill ångra regelns inställningar klickar du på knappen **Cancel Changes** (Avbryt inställningar).

Bild 5-25: List of PCs (Lista med datorer)

Bild 5-26: Add/Edit Service (Lägg till/redigera tjänst)

Fliken Applications and Gaming (Tillämpningar och spel)

Fliken Single Port Forwarding (Vidarebefordran av en port)

Single Port Forwarding (Vidarebefordran av en port)

Använd skärmbilden *Single Port Forwarding* (Vidarebefordran av en port) när du vill öppna en viss port så att användare på Internet kan se servrarna bakom gatewayen (t.ex. FTP- eller e-postservrar). När användare skickar den här typen av begäran till nätverket via Internet, vidarebefordrar gatewayen dem till rätt dator. Alla datorer vars port vidarebefordras bör ha sin DHCP-klientfunktion avaktiverad och ska ha en ny statisk IP-adress tilldelad till sig eftersom dess IP-adress kan ändras när DHCP-funktionen används.

- Port Map List (Portkartlista). Här kan du anpassa porttjänsten för dina tillämpningar.
    - Application (Tillämpning). Ange namnet på tillämpningen i motsvarande fält.
    - External Port (Extern port) och Internal Port (Intern port). Ange den externa och interna portens nummer.
    - Protocol (Protokoll). Välj det protokoll som du vill använda för varje tillämpning: **TCP** eller **UDP**.
    - IP Address (IP-adress): Ange IP-adressen till datorn.
    - Enabled (Aktiverad). Klicka på **Enabled** (Aktiverad) om du vill aktivera vidarebefordran för den valda tillämpningen.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.

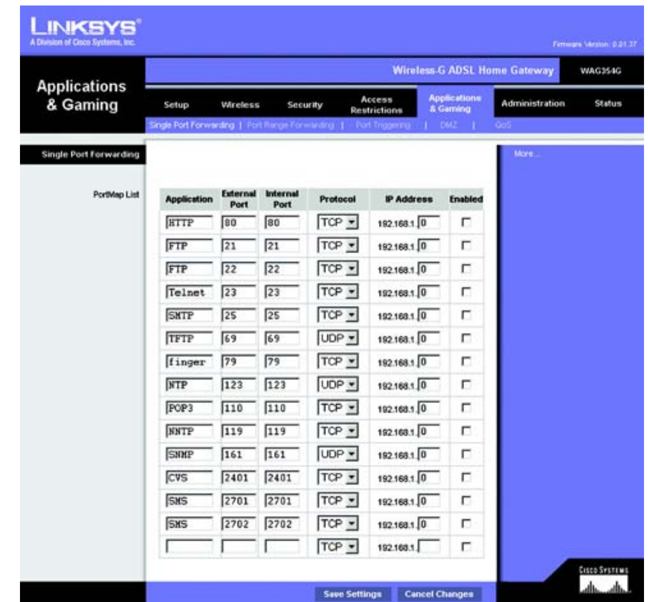


Bild 5-27: Single Port Forwarding (Vidarebefordran av en port)

Fliken Port Range Forwarding (Vidarebefordran av portintervall)

På skärmbilden *Port Range Forwarding* (Vidarebefordran av portintervall) anger du offentliga tjänster på nätverket, t.ex. webbservrar, ftp-servrar, e-postservrar eller andra specialiserade Internet-tillämpningar. (Specialiserade Internet-tillämpningar är tillämpningar som använder Internet-åtkomst till att utföra funktioner som videokonferenser eller onlinespel. Visa Internet-tillämpningar kräver ingen vidarebefordran.)

När användare skickar den här typen av begäran till nätverket via Internet, vidarebefordrar gatewayen dem till rätt dator. Alla datorer vars port vidarebefordras bör ha sin DHCP-klientfunktion avaktiverad och ska ha en ny statisk IP-adress tilldelad till sig eftersom dess IP-adress kan ändras när DHCP-funktionen används.

- Application (Tillämpning). Ange namnet på tillämpningen i motsvarande fält.
- Start och End (Slut). Ange start- och slutnummer för det portintervall som du vill vidarebefordra.
- Protocol (Protokoll). Välj det protokoll som du vill använda för varje tillämpning: **TCP**, **UDP** eller **Both**.
- IP Address (IP-adress): Ange IP-adressen till datorn.
- Enable (Aktivera). Markera kryssrutan **Enable** (Aktivera) för att aktivera vidarebefordran för den valda tillämpningen.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.

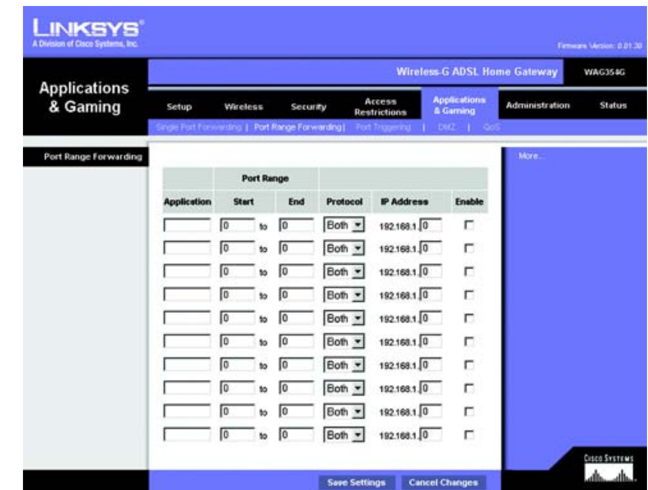


Bild 5-28: Port Range Forwarding (Vidarebefordran av portintervall)

Fliken Port Triggering (Portutlösare)

Den här funktionen används för särskilda tillämpningar som kan kräva att en port öppnas på begäran. För den här funktionen övervakar gatewayen utgående data för specifika portnummer. Gatewayen kommer ihåg IP-adressen för den dator som skickar en överföring som kräver information, så att när den begärda informationen återkommer genom gatewayen, dras informationen tillbaka till rätt dator via IP-adress och portanpassningsregler.

- Application (Tillämpning). Ange det namn som du vill ge varje tillämpning.
- Triggered Range (Utlöst intervall). Ange start- och slutportnummer för det utlösta intervallet.
- Forwarded Range (Vidarebefordrat intervall). Ange start- och slutportnummer för det vidarebefordrade intervallet.
- Enable (Aktivera). Markera kryssrutan **Enable** (Aktivera) för att aktivera portutlösare för den valda tillämpningen.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.

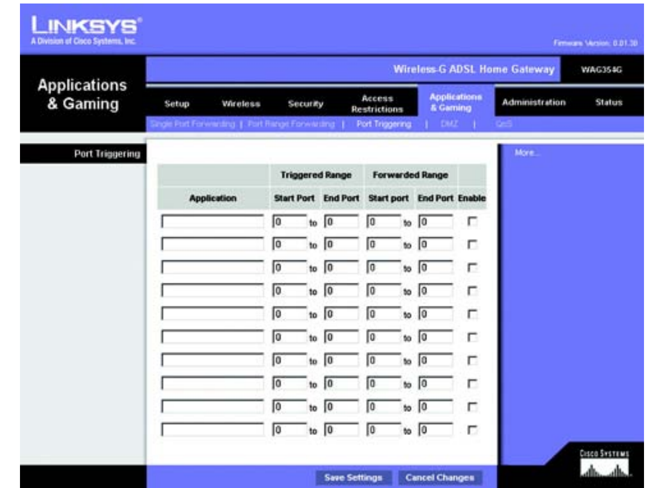


Bild 5-29: Port Triggering (Portutlösare)

Fliken DMZ

På skärmbilden *DMZ* kan en lokal användare exponeras för Internet för användning av en särskild tjänst, t.ex. Internet-spel och videokonferenser via DMZ Hosting. DMZ Hosting vidarebefordrar alla portar för en dator samtidigt, vilket skiljer sig från vidarebefordran av portintervall som högst kan vidarebefordra 10 portintervall.

- DMZ Hosting. Med den här funktionen kan en lokal användare exponeras för Internet för användning av en särskild tjänst, t.ex. Internet-spel och videokonferenser. Om du vill använda den här funktionen väljer du **Enable** (Aktivera). Om du vill avaktivera DMZ väljer du **Disable** (Avaktivera).

- DMZ Host IP Address (IP-adress för DMZ-värd). Om du vill exponera en dator anger du datorns IP-adress. Om du vill hämta IP-adressen för en dator läser du "Bilaga C: Hitta MAC-adress och IP-adress för Ethernet-kortet".

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.



Bild 5-30: DMZ

Fliken QoS

QoS

QoS-tjänsten (Quality of Service) säkerställer bättre tjänst för högprioriterad nätverkstrafik, t.ex. krävande realtidstillämpningar som Internet-telefoni eller videokonferens.

Enabled/Disabled (Aktiverad/avaktiverad) Om du vill använda QoS väljer du **Enable** (Aktiverad) **I** annat fall behåller du standardvärdet **Disabled** (Avaktiverad).

Application-based QoS (Tillämpningsbaserad QoS)

Den här funktionen hanterar information som den sänds och tas emot. Beroende på inställningarna på skärmbilden *QoS,* tilldelar den här funktionen information en hög eller låg prioritet för de fem förinställda tillämpningarna och ytterligare tre tillämpningar som du kan ange.

High priority/Medium priority/Low priority (Hög/medelhög/låg prioritet). För varje tillämpning väljer du **High priority** (Hög prioritet) (trafik i den här kön delar på 60 % av den totala bandbredden), **Medium priority** (Medelhög prioritet) (trafik i den här kön delar på 18 % av den totala bandbredden) eller **Low priority** (Låg prioritet) (trafik i den här kön delar på 1 % av den totala bandbredden).

FTP (File Transfer Protocol). Ett protokoll som används för att överföra filer över ett TCP/IP-nätverk (Internet, UNIX, osv.). Exempel: efter att ha utvecklat HTML-sidorna för en webbplats på en lokal dator överförs de vanligen till webbservern via FTP.

HTTP (HyperText Transport Protocol). De kommunikationsprotokoll som används för att ansluta till servrar på webben. Dess primära funktion är att upprätta en anslutning med en webbserver och överföra HTML-sidor till klientwebbläsaren.

Telnet. Ett terminalemuleringsprotokoll som ofta används på Internet och TCP/IP-baserade nätverk. Med det kan en användare på en terminal eller dator logga in på en fjärrenhet och köra ett program.

SMTP (Simple Mail Transfer Protocol). Standardprotokollet för e-post på Internet. Det är ett TCP/IP-protokoll som definierar det meddelandeformat och den meddelandeöverföringsagent (MTA) som lagrar och vidarebefordrar posten.

POP3 (Post Office Protocol 3). En standardpostserver som ofta används på Internet. Den utgör ett meddelandelager som förvarar inkommande e-post tills användare loggar in och hämtar den. POP3 är ett enkelt system med få valbara funktioner. Alla väntande meddelanden och bilagor hämtas samtidigt. POP3 använder meddelandeprotokollet SMTP.

Specific Port# (Specifikt portnummer). Du kan lägga till ytterligare tre tillämpningar genom att ange respektive portnummer i de här fälten.

När du är klar med den här skärmbilden klickar du på knappen **Save Settings** (Spara inställningar) för att spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avsluta utan att spara ändringarna.

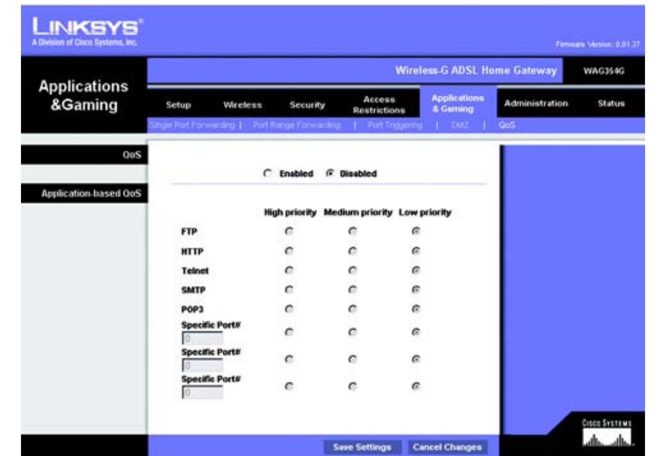


Bild 5-31: QoS

Fliken Administration

Fliken Management (Hantering)

På skärmbilden *Management* (Hantering) kan du ändra gatewayens åtkomstinställningar samt konfigurera hanteringen av SNMP (Simple Network Management Protocol), UPnP (Universal Plug and Play), IGMP (Internet Group Multicast Protocol)-Proxy och WLAN.

Gateway Access (Gateway-åtkomst)

Local Gateway Access (Lokal gatewayåtkomst). För att säkerställa gatewayens säkerhet ombeds du ange ditt lösenord när du ansluter till gatewayens webbaserade verktyg. Standardanvändarnamnet och lösenordet är **admin**.

- Gateway Userlist (Användarlistan för gatewayen). Välj numret för användaren i listrutan.
- Gateway Username (Användarnamn för gatewayen). Ange standardnamnet, **admin.** Det rekommenderas att du byter standardanvändarnamnet till ett eget.
- Gateway Password (Lösenord för gatewayen). Det rekommenderas att du byter standardlösenordet, **admin**, till ett eget.
- Ange det på nytt för att bekräfta. Ange gatewayens nya lösenord på nytt för att bekräfta det.

Remote Gateway Access (Fjärråtkomst av gatewayen). Med den här funktionen kan du komma åt gatewayen från en fjärrplats, via Internet.

- Remote Management (Fjärrhantering). Med den här funktionen kan du hantera gatewayen från en fjärrplats, via Internet. Om du vill aktivera funktionen klickar du på **Enable** (Aktivera).



VIKTIGT! Här kan alla som känner till lösenordet konfigurera gatewayen från en annan plats på Internet.

- Management Port (Hanteringsport). Ange det portnummer som kommer att användas för fjärråtkomst till gatewayen.
- Allowed IP (Tillåtna IP). Ange de IP-adresser som tillåts fjärrhantera gatewayen. Om du vill tillåta alla IP-adresser utan begränsningar väljer du **All** (Alla) Om du vill ange en IP-adress väljer du **IP address** (IP-adress) och anger sedan IP-adressen i fälten. Om du vill ange ett intervall med IP-adresser väljer du **IP range** (IP-intervall) och anger sedan IP-adressintervallet i fälten.

Remote Upgrade (Fjärruppgradering). Med den här funktionen kan du uppgradera gatewayens fasta programvara via en TFTP-server. Om du vill aktivera funktionen klickar du på **Enable** (Aktivera).

Bild 5-32: Management (Hantering)

Bild 5-33: Allowed IP (Tillåtna IP) - IP Range (IP-intervall)

SNMP

SNMP är ett populärt protokoll för nätverksövervakning och hantering. Om du vill aktivera protokollet klickar du på **Enabled** (Aktiverat). Om du vill avaktivera protokollet klickar du på **Disabled** (Avaktiverat)

Om du aktiverar protokollet anger du sedan de IP-adresser som tillåts ha SNMP-åtkomst. Välj **All** (Alla) om du vill tillåta alla IP-adresser utan begränsningar, **IP address** (IP-adress) om du vill ange en IP-adress eller **IP range** (IP-intervall) om du vill ange ett intervall med IP-adresser.

- Device Name (Enhetsnamn): Ange namnet på gatewayen.
- SNMP v1/v2: Get Community (Hämta mötesplats). Ange lösenordet som medger läsåtkomst till gatewayens SNMP-information.
- Set Community (Ange mötesplats). Ange lösenordet som medger läs-/skrivåtkomst till gatewayens SNMP-information.
- Trap Management (Felhantering): Trap to (Fel till). Ange IP-adressen för fjärrvärddatorn som ska ta emot felmeddelanden.

UPnP

UPnP gör att Windows Me och XP kan konfigurera gatewayen automatiskt för olika Internet-tillämpningar som spel och videokonferenser.

- UPnP. Om du vill aktivera UPnP klickar du på **Enable** (Aktivera) I annat fall klickar du på **Disable** (Avaktivera).

IGMP-Proxy

Om din multimediatillämpning eller -enhet inte fungerar korrekt bakom gatewayen kan du aktivera IGMP-Proxy och tillåta multicasttrafik genom gatewayen.

- IGMP-proxy. Om du vill använda den här funktionen väljer du **Enable** (Aktivera). I annat fall väljer du **Disable** (Avaktivera).

WLAN

- Hantering via WLAN. Med den här funktionen kan gatewayen hanteras från en trådlös dator i det lokala nätverket när den loggar in på gatewayens webbaserade verktyg.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.

Fliken Reporting (Rapportering)

På skärmbilden *Reporting* (Rapportering) visas en logg med alla inkommande och utgående URL-adresser och IP-adresser för Internet-anslutningen. Här finns också loggar för VPN och brandväggshändelser.



Bild 5-34: Reporting (Rapportering)

Reporting (Rapportering)

- Log (Logg). Om du vill aktivera loggrapportering klickar du på **Enabled** (Aktiverad).
- Logviewer IP Address (IP-adress för Logviewer). Ange IP-adressen för den dator som ska ta emot loggar. Du måste ha programvaran Logviewer för att visa dessa loggar. Denna kostnadsfria programvara kan hämtas från www.linksys.com.

Email Alerts (Varningsmeddelanden via e-post)

- Email Alerts (Varningsmeddelanden via e-post). Om du vill använda den här funktionen väljer du **Enable** (Aktivera).
- Denial of Service Thresholds (DoS-gränsvärden). Ange antalet DoS-attacker som ska utlösa ett varningsmeddelande via e-post.
- SMTP Mail Server (SMTP-postserver). Ange IP-adressen till SMTP-servern.
- E-Mail Address for Alert Logs (E-postadress för varningsloggar). Ange den e-postadress som ska ta emot varningsloggar.
- Return E-Mail address (E-postadress för svar). Ange svarsadressen för varningsmeddelandena via e-post.

Om du vill visa loggarna klickar du på knappen **View Logs** (Visa loggar). En ny skärmbild visas. I listrutan kan du välja vilken logg som du vill visa. Klicka på knappen **Clear** (Rensa) om du vill rensa logginformationen. Klicka på knappen **pageRefresh** (Uppdatera sida) om du vill uppdatera informationen. Klicka på knappen **Previous Page** (Föregående sida) om du vill gå till den föregående sidan med information. Klicka på knappen **Next Page** (Nästa sida) om du vill gå till nästa sida med information.



Bild 5-35: System Log (Systemlogg)

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.

Fliken Diagnostics (Diagnostik)

Ping Test (Pingtest)

Ping Test Parameters (Parametrar för pingtest)

- Ping Target IP (Mål-IP för ping). Ange den IP-adress som du vill pinga. Detta kan vara en lokal (LAN) IP-adress eller en Internet-IP-adress (WAN).
- Ping Size (Pingstorlek). Ange storleken på paketet.
- Number of Pings (Antal ping). Ange antalet gånger som du vill pinga.
- Ping Interval (Pingintervall). Ange pingintervallet (hur ofta mål-IP-adressen ska pingas) i millisekunder.
- Ping Timeout (Tidsgräns för ping). Ange tidsgränsen för ping (efter hur lång tid ping-försöket ska avbrytas) i millisekunder.

Klicka på knappen **Start Test** (Starta test) för att starta pingtestet.

- Ping Result (Resultat för ping). Här visas resultatet av pingtestet.

När du är klar med ändringarna på den här fliken klickar du på **Save Settings** (Spara inställningar) om du vill spara ändringarna eller på **Cancel Changes** (Avbryt ändringar) om du vill avbryta ändringarna.



Bild 5-36: Ping Test (Pingtest)

Fliken Backup&Restore (Säkerhetskopiering och återställning)

På den här fliken kan du säkerhetskopiera och återställa gatewayens konfigurationsfil.

Backup Configuration (Konfiguration av säkerhetskopiering)

Om du vill säkerhetskopiera gatewayens konfigurationsfil klickar du på knappen **Backup** (Säkerhetskopiera). Följ sedan anvisningarna på skärmen.

Restore Configuration (Återställ konfiguration)

Om du vill återställa gatewayens konfigurationsfil klickar du på knappen **Browse** (Bläddra). Leta sedan upp filen genom att följa anvisningarna på skärmen. När du har markerat filen klickar du på knappen **Restore** (Återställ).

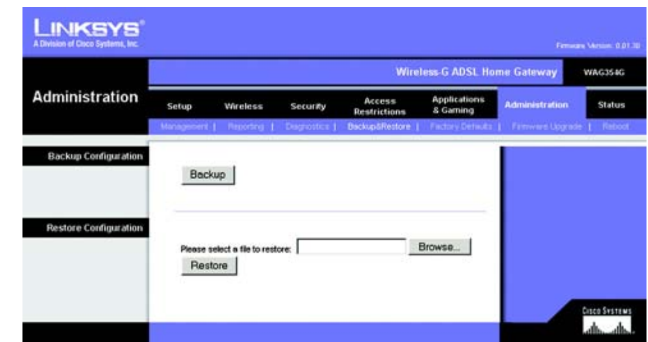


Bild 5-37: Backup&Restore (Säkerhetskopiering och återställning)

Fliken Factory Defaults (Fabriksinställningar)



Bild 5-38: Factory Defaults (Fabriksinställningar)

Restore Factory Defaults (Återställ fabriksinställningar). Om du vill återställa gatewayen till fabriksinställningarna och förlora alla dina inställningar klickar du på **Yes** (Ja).

Om du vill påbörja återställningsprocessen klickar du på knappen **Save Settings** (Spara inställningar) för att spara ändringarna eller klickar på **Cancel Changes** (Avbryt inställningar) om du inte vill spara dem.

Fliken Firmware Upgrade (Uppgradera fast programvara)

Du kan uppgradera gatewayens fasta programvara från det lokala nätverket.

Upgrade from LAN (Uppgradera från LAN)



Bild 5-39: Firmware Upgrade (Uppgradera fast programvara)

Så här uppgraderar du gatewayens fasta programvara från det lokala nätverket:

1. Ladda ned filen med uppdateringen av gatewayens fasta programvara från www.linksys.com/international.
2. Packa upp filen i datorn.
3. Klicka på knappen **Browse** (Bläddra) för att söka efter uppgraderingsfilen.
4. Dubbelklicka på den fil du hämtade och packade upp.
5. Klicka på knappen **Upgrade** (uppgradera) och följ anvisningarna på skärmen.

Om du vill avbryta uppgraderingen klickar du på knappen **Cancel Upgrade** (Avbryt uppgradering).

Fliken Reboot (Omstart)

På den här skärmbilden kan du göra en mjuk eller hård omstart av gatewayen. I de flesta fall bör du göra en hård omstart. Den mjuka omstarten likar det sätt du startar om datorn utan att först stänga av den.

Reboot (Omstart)

Reboot Mode (Omstartsläge). Om du vill starta om gatewayen väljer du **Hard** (Hård) eller **Soft** (Mjuk). Välj **Hard** (Hård) om du vill starta om gatewayen genom att stänga av och slå på strömmen eller **Soft** (Mjuk) om du vill starta om den med strömmen påslagen.

Påbörja omstartsprocessen genom att klicka på knappen **Save Settings** (Spara inställningar). När en skärmbild visas med en fråga om du vill starta om gatewayen klickar du på **OK.**

Klicka på knappen **Cancel Changes** (Avbryt ändringar) om du vill avbryta omstarten.



Bild 5-40: Reboot (Omstart)

Fliken Status

Fliken Gateway

På den här skärmbilden visas information om gatewayen och dess Internet-anslutning.

Gateway Information (Gatewayinformation)

Här visas gatewayens fasta programvaruversion, MAC-adress och aktuell tid.

Internet Connection (Internet-anslutning)

Här visas följande information: anslutningen, inloggningstyp, gränssnitt, IP-adress, nätmask, standardgateway, IP-adresserna till DNS-server 1, 2 och 3 och WINS-adress.



Bild 5-41: Gateway

DHCP Renew (Förnya DHCP). Klicka på knappen **DHCP Renew** (Förnya DHCP) om du vill ersätta gatewayens aktuella IP-adress med en ny IP-adress.

DHCP Release (Frigör DHCP). Klicka på knappen **DHCP Release** (Frigör DHCP) om du vill ta bort gatewayens aktuella IP-adress.

Klicka på knappen **Refresh** (Uppdatera) om du vill uppdatera informationen som visas.

Fliken Local Network (Lokalt nätverk)

Den information om lokalt nätverk som visas är den lokala Mac-adressen, IP-adressen, nätmasken, DHCP-server, start- och slut-IP-adresser. Om du vill visa DHCP-klienttabellen klickar du på knappen **DHCP Clients Table** (DHCP-klienttabell). Om du vill visa ARP-/RARP-tabellen klickar du på knappen **ARP/RARP Table** (ARP-/RARP-tabell).

DHCP Clients Table (DHCP-klienttabell). I tabellen DHCP Active IP (Aktivt DHCP-ID) visas aktuella DHCP-klientdata. Här visas datorns namn, IP-adress, MAC-adress och förfallodatum för den dynamiska IP-adressen för de trådlösa klienterna som använder DHCP-servern. (Dessa data lagras i ett tillfälligt minne och ändras med jämna mellanrum.) Klicka på knappen **Refresh** (Uppdatera) om du vill uppdatera informationen som visas. Om du vill ta bort en klient från DHCP-servern markerar du klienten och klickar sedan på knappen **Delete** (Ta bort). Klicka på knappen **Close** (Stäng) om du vill gå tillbaka till skärmbilden *Local Network* (Lokalt nätverk).

ARP/RARP Table (ARP-/RARP-tabell). I den här tabellen visas aktuella data för de lokala nätverksklienterna som har skickat en ARP-begäran till gatewayen. Här visas deras IP-adresser och MAC-adresser. (Dessa data lagras i ett tillfälligt minne och ändras med jämna mellanrum.) En ARP-begäran är en begäran som skickas av gatewayen som ber klienter med IP-adresser om deras MAC-adresser så att gatewayen kan koppla IP-adresser till MAC-adresser. RARP är det omvända mot ARP. Klicka på knappen **Refresh** (Uppdatera) om du vill uppdatera informationen som visas. Klicka på knappen **Close** (Stäng) om du vill gå tillbaka till skärmbilden *Local Network* (Lokalt nätverk).

Klicka på knappen **Refresh** (Uppdatera) om du vill uppdatera informationen som visas.



Bild 5-42: Local Network (Lokalt nätverk)

DHCP Active IP Table

DHCP Server IP Address: 192.168.1.1 Refresh

Client Host Name	IP Address	MAC Address	Expires	
None	None	None	None	Delete

Close

Bild 5-43: Tabellen DHCP Active IP (Aktivt DHCP-ID)

ARP/RARP Table Close

IP Address	MAC Address	
192.168.1.64	00:D0:B7:B6:46:BA	Refresh

Bild 5-44: ARP/RARP Table (ARP-/RARP-tabell)

Fliken Wireless (Trådlöst)

Den trådlösa nätverksinformation som visas är den trådlösa fasta programvaruversionen, MAC-adress, läge, SSID, DHCP-server, kanal och krypteringsfunktion.

Klicka på knappen **Wireless Clients Connected** (Anslutna trådlösa klienter) om du vill visa en lista med trådlösa klienter som är anslutna till gatewayen, tillsammans med deras datornamn, IP-adresser och MAC-adresser. Klicka på knappen **Refresh** (Uppdatera) om du vill uppdatera informationen som visas. Klicka på knappen **Close** (Stäng) om du vill gå tillbaka till skärmbilden *Wireless* (Trådlöst).

Klicka på knappen **Refresh** (Uppdatera) om du vill uppdatera informationen som visas.



Bild 5-45: Wireless (Trådlöst)



Bild 5-46: Networked Computers (Nätverksanslutna datorer)

Fliken DSL Connection (DSL-anslutning)

På den här skärmbilden visas information om DSL-anslutningen och PVC-anslutningen.

DSL Status (DSL-status)

Här visas följande information: DSL-status, DSL-moduleringsläge, DSL-sökvägsläge, nedströmshastighet, uppströmshastighet, nedströmsmarginal, uppströmsmarginal, nedströmslinjeförstärkning, uppströmslinjeförstärkning, nedströms sändningseffekt och uppströms sändningseffekt.

PVC Connection (PVC-anslutning)

Här visas följande information: inkapsling, multiplexing, QoS, Pcr-hastighet, Scr-hastighet, automatisk avkänning, VPI, VCI, aktiveringsstatus och PVC-status.

Klicka på knappen **Refresh** (Uppdatera) om du vill uppdatera informationen som visas.



Bild 5-47: DSL Connection (DSL-anslutning)

Bilaga A: Felsökning

Den här bilagan består av två delar: "Lösningar på vanliga problem" och "Vanliga frågor". Här föreslås möjliga lösningar på problem som kan inträffa vid installation och drift av gatewayen. Läs beskrivningarna nedan när du vill få hjälp med att lösa ett problem. Om du inte hittar svaret här kan du i stället besöka Linksys internationella webbplats på www.linksys.com/international.

Lösningar på vanliga problem

1. Jag behöver ange en statisk IP-adress för en dator.

Så här tilldelar du en statisk IP-adress till en dator:

- För Windows 98 och Me:
  1. Klicka på **Start**, **Inställningar** och **Kontrollpanelen**. Dubbelklicka på **Nätverk**.
  2. I rutan Följande nätverkskomponenter finns installerade, väljer du TCP/IP för aktuell Ethernet-adapter. Om du endast har en Ethernet-adapter installerad visas endast en TCP/IP-rad utan koppling till en Ethernet-adapter. Markera den och klicka på knappen Egenskaper.
  3. I rutan Egenskaper för TCP/IP väljer du fliken IP-adress och väljer Ange en IP-adress. Ange en unik IP-adress som inte används av någon annan dator i det nätverk som är anslutet till gatewayen. Se till att varje IP-adress är unik för varje dator eller nätverksenhet.
  4. Klicka på fliken **Gateway** och under Ny gateway anger du sedan 192.168.1.1, vilket är den förvalda IP-adressen för gatewayen. Bekräfta genom att klicka på Lägg till.
  5. Klicka på fliken **DNS** och se till att alternativet Aktivera DNS är markerat. Ange värd- och domännamn (t ex Jan för värd och hem för domän). Ange den DNS-uppgift som tillhandahålls av Internet-leverantören. Om Internet-leverantören inte har tillhandahållit någon IP-adress för DNS kontaktar du Internet-leverantören eller besöker deras webbplats och inhämtar informationen.
  6. Klicka på **OK** i dialogrutan för TCP/IP-egenskaper och klicka på Stäng eller OK i dialogrutan Nätverk.
  7. Starta om datorn när du blir uppmanad.
- För Windows 2000:
  1. Klicka på **Start**, **Inställningar** och **Kontrollpanelen**. Dubbelklicka på **Nätverksanslutningar**.
  2. Högerklicka på den anslutning till lokalt nätverk som är kopplad till den Ethernet-adapter du använder och välj alternativet Egenskaper.
  3. I rutan Markerade komponenter används av anslutningen, markerar du Internet Protocol (TCP/IP) och klickar på knappen **Egenskaper**. Markera alternativet **Använd följande IP-adress.**
  4. Ange en unik IP-adress som inte används av någon annan dator i det nätverk som är anslutet till gatewayen.
  5. Ange nätmasken 255.255.255.0.
  6. Ange standard-gateway 192.168.1.1 (gatewayens förvalda IP-adress).

7. I nedre delen av dialogrutan markerar du Använd följande DNS-serveradresser, och anger Önskad DNS-server och Alternativ DNS-server (tillhandahålls av Internet-leverantören). Kontakta Internet-leverantören eller besök deras webbplats om du vill ha mer information.
8. Klicka på **OK** i dialogrutan Egenskaper för Internet Protocol (TCP/IP) och klicka på **OK** i dialogrutan Egenskaper för Anslutning till lokalt nätverk.
9. Starta om datorn om du blir uppmanad.

- För Windows XP:

  I följande anvisningar antas att du kör Windows XP med standardgränssnitt. Om du använder klassiskt gränssnitt (där ikoner och menyer ser ut som i tidigare Windows-versioner) följer du anvisningarna för Windows 2000.

  1. Klicka på **Start** och **Kontrollpanelen.**
  2. Klicka på ikonen **Nätverk och Internet-anslutningar** och sedan på ikonen **Nätverksanslutningar.**
  3. Högerklicka på den **anslutning till lokalt nätverk** som är kopplad till den Ethernet-adapter du använder och välj alternativet Egenskaper.
  4. I rutan **Den här anslutningen använder följande objekt** markerar du **Internet Protocol (TCP/IP).** Klicka på **Egenskaper.**
  5. Ange en unik IP-adress som inte används av någon annan dator i det nätverk som är anslutet till gatewayen.
  6. Ange nätmasken 255.255.255.0.
  7. Ange standard-gateway 192.168.1.1 (gatewayens förvalda IP-adress).
  8. I nedre delen av dialogrutan markerar du Använd följande DNS-serveradresser, och anger Önskad DNS-server och Alternativ DNS-server (tillhandahålls av Internet-leverantören). Kontakta Internet-leverantören eller besök deras webbplats om du vill ha mer information.
  9. Klicka på **OK** i dialogrutan Egenskaper för Internet Protocol (TCP/IP). Klicka på **OK** i dialogrutan Egenskaper för Lokalt nätverk.

2. Jag vill testa min Internet-anslutning.

A. Kontrollera TCP/IP-inställningarna.

För Windows 98, Me, 2000 och XP:

- Mer information finns i Windows-hjälpen. Se till att Erhåll en IP-adress automatiskt är markerat i inställningarna.

För Windows NT 4.0:

- Klicka på **Start**, **Inställningar** och **Kontrollpanelen.** Dubbelklicka på ikonen **Nätverk.**
- Klicka på fliken Protokoll och dubbelklicka på TCP/IP Protocol.
- När dialogrutan visas kontrollerar du att du har valt rätt kort för Ethernet-adaptern och ställer in det på **Hämta en IP-adress** från en DHCP-server.
- Klicka på **OK** i dialogrutan Egenskaper för TCP/IP Protocol och klicka på **Stäng** i dialogrutan Nätverk.
- Starta om datorn om du blir uppmanad.

B. Öppna en kommandoprompt.

För Windows 98 och Me:

- Klicka på **Start** och **Kör.** Skriv kommandot i fältet Öppna. Tryck på **Enter** eller klicka på **OK.**

För Windows NT, 2000 och XP:

- Klicka på **Start** och **Kör.** I fältet Öppna skriver du cmd. Tryck på **Enter** eller klicka på **OK**. Vid kommandoprompten skriver du ping 192.168.1.1 och trycker på Enter.
- Om du får ett svar kommunicerar datorn med gatewayen.
- Om du INTE får ett svar bör du kontrollera kabeln och se till att Erhåll en IP-adress automatiskt är markerat i TCP/IP-inställningarna för Ethernet-adaptern.

C. Vid kommandoprompten skriver du ping följt av Internet- eller WAN-IP-adressen och trycker på **Enter**. Internet- eller WAN-IP-adressen hittar du på sidan Status i gatewayens webbaserade verktyg. Om Internet- eller WAN-IP-adressen till exempel är 1.2.3.4, skriver du ping 1.2.3.4 och trycker på Enter.

- Om du får ett svar är datorn ansluten till gatewayen.
- Om du INTE får ett svar kan du pröva ping-kommandot från en annan dator för att verifiera att den första datorn inte är orsaken till problemet.

D. Vid kommandoprompten skriver du ping www.yahoo.com och trycker på **Enter.**

- Om du får ett svar är datorn ansluten till Internet. Om du inte kan öppna en webbsida kan du pröva ping-kommandot från en annan dator för att verifiera att den första datorn inte är orsaken till problemet.
- Om du INTE får ett svar kan det vara fel på anslutningen. Pröva ping-kommandot från en annan dator för att verifiera att den första datorn inte är orsaken till problemet.

3. Jag får inte en IP-adress på Internet med min Internet-anslutning.

- Se avsnittet "Problem 2: Jag vill testa min Internet-anslutning" om du vill kontrollera att en anslutning har upprättats.
    1. Se till att du använder rätt inställningar för Internet-anslutningen. Kontakta Internet-leverantören och kontrollera om Internet-anslutningen är av typen RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE eller RFC 2364 PPPoA. Se avsnittet om konfiguration i "Kapitel 5: Konfigurera Wireless-G-ADSL-gatewayen för hemmet" om du vill ha mer information om inställningar för Internet-anslutning.
    2. Se till att du har rätt kabel. Kontrollera att ADSL-lysdioden på gatewayen lyser med fast sken.
    3. Se till att kabeln från gatewayens ADSL-port är ansluten till vägguttaget för ADSL-tjänstens linje. Kontrollera att en giltig IP-adress från Internet-leverantören visas på sidan Status i gatewayens webbaserade verktyg.
    4. Stäng av datorn och gatewayen. Vänta i 30 sekunder och starta sedan gatewayen och datorn. Se efter på fliken Status i gatewayens webbaserade verktyg att du erhållit en IP-adress.

4. Jag kan inte få åtkomst till sidan Setup (Konfigurera) i gatewayens webbaserade verktyg.

- Se avsnittet "Problem 2: Jag vill testa min Internet-anslutning" om du vill kontrollera att datorn är rätt ansluten till gatewayen.
    1. Se avsnittet "Bilaga C: Hitta MAC- och IP-adressen för Ethernet-adaptern" om du vill kontrollera att datorn har en IP-adress, nätmask, gateway och DNS.
    2. Ange en statisk IP-adress i systemet. Se avsnittet "Problem 1: Jag behöver ange en statisk IP-adress".

3. Se avsnittet "Problem 10: Jag är en PPPoE-användare och behöver ta bort proxy-inställningarna eller dialogrutan för uppringning."

5. Jag får inte mitt VPN-nätverk (Virtual Private Network) att fungera via gatewayen.

Öppna gatewayens webbgränssnitt genom att gå till http://192.168.1.1 eller gatewayens IP-adress och visa fliken Security (Säkerhet). Kontrollera att IPsec passthrough (IPsec-genomströmning) och/eller PPTP pass-through (PPTP-genomströmning) är aktiverat.

- VPN-nätverk där IPSec med ESP-autentisering (Encapsulation Security Payload, även kallat protokoll 50) används fungerar utmärkt. Minst en IPSec-session kan användas via gatewayen. Samtidiga IPSec-sessioner kan dock vara möjliga, beroende på VPN-nätverkets utformning.
- VPN-nätverk där IPSec och AH (Authentication Header, även kallat protokoll 51) används är inkompatibla med gatewayen. AH har begränsningar på grund av viss inkompatibilitet med NAT-standarden.
- Ändra IP-adress för gatewayen till ett annat nät för att undvika en konflikt mellan VPN-IP-adressen och den lokala IP-adressen. Om till exempel VPN-servern tilldelar IP-adressen 192.168.1.X (X är en siffra mellan 1 och 254) och det lokala nätverkets IP-adress är 192.168.1.X (X är samma siffra som används i VPN-IP-adressen), får gatewayen svårigheter att dirigera information till rätt plats. Du bör kunna lösa problemet genom att ändra gatewayens IP-adress till 192.168.2.1. Ändra gatewayens IP-adress via fliken Setup (Konfigurera) i webbgränssnittet.
- Om du har tilldelat en statisk IP-adress till en dator eller nätverksenhet i nätverket måste du ändra dess IP-adress på samma sätt till 192.168.2.Y (där Y är en siffra mellan 1 och 254). Observera att varje IP-adress måste vara unik i nätverket.
- VPN-nätverket kan fordra att paket för port 500/UDP överförs till den dator som ansluter till IPSec-servern. Se avsnittet "Problem 7: Jag behöver konfigurera en värd för Internet-spel eller använda andra Internet-program".
- Gå till Linksys internationella webbplats på www.linksys.com/international om du vill ha mer information.

6. Jag behöver konfigurera en server bakom gatewayen och göra den åtkomlig för allmänheten.

Om du vill använda en server såsom en webb-, ftp- eller e-postserver måste du känna till vilka respektive portnummer de använder. Port 80 (HTTP) används till exempel för webb, port 21 (FTP) för FTP och port 25 (SMTP utgående) samt port 110 (POP3 inkommande) för e-post. Du kan få mer information genom att granska dokumentationen för den server du har installerat.

- Följ de här anvisningarna när du vill konfigurera vidarebefordran av portar via gatewayens webbaserade verktyg. Vi kommer här att konfigurera webb-, ftp- och e-postservrar.
  1. Öppna gatewayens webbaserade verktyg genom att gå till http://192.168.1.1 eller gatewayens IP-adress. Visa fliken Applications and Gaming => Port Range Forwarding (Program och spel => Vidarebefordran av portintervall).
  2. Ange ett namn som du vill använda för det anpassade programmet.
  3. Ange det externa portintervallet för den tjänst du använder. Om du till exempel har en webbserver anger du intervallet 80 till 80.
  4. Kontrollera vilket protokoll du använder, TCP och/eller UDP.

5. Ange IP-adressen för den dator eller nätverksenhet som du vill att portens server ska gå till. Om till exempel IP-adressen för webbserverns Ethernet-adapter är 192.168.1.100, anger du 100 i fältet. Se avsnittet "Bilaga C: Hitta MAC- och IP-adressen för Ethernet-adaptern" för information om hur du får en IP-adress.
6. Kontrollera att de porttjänster som du vill använda är aktiverade. Studera exemplet nedan:

Anpassat program	Extern port	TCP	UDP	IP-adress	Aktivera
Webbserver	80 till 80	X		192.168.1.100	X
FTP-server	21 till 21	X		192.168.1.101	X
SMTP (utgående)	25 till 25	X		192.168.1.102	X
POP3 (inkommande)	110 till 110	X		192.168.1.102	X

När du är klar med konfigureringen klickar du på **Save Settings** (Spara inställningar).

7. Jag behöver konfigurera en värd för Internet-spel eller använda andra Internet-program.

Om du vill spela Internet-spel eller använda Internet-program, kan du i de flesta fall göra det utan att konfigurera någon vidarebefordran av portar eller DMZ-värd. Det kan förekomma fall där du vill fungera som värd för ett Internet-spel eller Internet-program. Då måste du konfigurera gatewayen så att den skickar inkommande paket eller data till en viss dator. Detta gäller även de Internet-program som du använder. Det bästa sättet att få information om vilka porttjänster du ska använda är att gå till webbplatsen för det Internet-spel/-program som du vill använda. Följ anvisningarna för hur du konfigurerar en värd för ett Internet-spel eller använder ett visst Internet-program:

1. Öppna gatewayens webbgränssnitt genom att gå till http://192.168.1.1 eller gatewayens IP-adress. Visa fliken Applications and Gaming => Port Range Forwarding (Program och spel => Vidarebefordran av portintervall).
2. Ange ett namn som du vill använda för det anpassade programmet.
3. Ange det externa portintervallet för den tjänst du använder. Om du till exempel vill fungera som värd för Unreal Tournament (UT) anger du intervallet 7777 till 27900.
4. Kontrollera vilket protokoll du använder, TCP och/eller UDP.
5. Ange IP-adressen för den dator eller nätverksenhet som du vill att portens server ska gå till. Om till exempel IP-adressen för webbserverns Ethernet-adapter är 192.168.1.100, anger du 100 i fältet. Se avsnittet "Bilaga C: Hitta MAC- och IP-adressen för Ethernet-adaptern" för information om hur du får en IP-adress.
6. Kontrollera at de porttjänster som du vill använda är aktiverade. Studera exemplet nedan:

Anpassat program	Extern port	TCP	UDP	IP-adress	Aktivera
UT	7777 till 27900	X	X	192.168.1.100	X
Halflife	27015 till 27015	X	X	192.168.1.105	X
PC Anywhere	5631 till 5631		X	192.168.1.102	X
VPN IPSEC	500 till 500		X	192.168.1.100	X

När du är klar med konfigureringen klickar du på **Save Settings** (Spara inställningar).

*8. **Internet-spelet, -servern eller -programmet fungerar inte.***

Om du har svårigheter att få Internet-spel, -servrar eller -program att fungera på rätt sätt kan du överväga att göra en dator synlig mot Internet som en DMZ-värd (DeMilitarized Zone). Det här alternativet kan användas när ett program fordrar för många portar eller när du inte är säker på vilken port en tjänst använder. Se till att du avaktiverar alla uppgifter om vidarebefordran om du vill konfigurera en DMZ-värd, eftersom vidarebefordran har högre prioritet än en DMZ-värd. (Med andra ord så kontrolleras de data som anländer till gatewayen först mot inställningarna för vidarebefordran. Om det portnummer som data inkommer från inte är konfigurerat för vidarebefordran skickas data till den dator eller nätverksenhet som du konfigurerar som DMZ-värd.)

- Följ anvisningarna nedan för hur du konfigurerar en DMZ-värd:
  1. Öppna gatewayens webbaserade verktyg genom att gå till http://192.168.1.1 eller gatewayens IP-adress. Visa fliken Applications and Gaming => DMZ (Program och spel => DMZ). Klicka på Enabled (Aktiverad) och ange datorns IP-adress.
  2. Kontrollera sidorna för vidarebefordran av portar och avaktivera eller ta bort de poster som du har angett för vidarebefordran. Behåll informationen om du skulle vilja använda den vid ett senare tillfälle.
- När du är klar med konfigureringen klickar du på **Save Settings** (Spara inställningar).

*9. **Jag har glömt mitt lösenord, eller jag uppmanas att ange lösenordet varje gång jag ska spara inställningarna för gatewayen.***

- Återställ gatewayen till fabriksinställningarna genom att trycka på knappen Reset (återställ) i 10 sekunder och sedan släppa den. Om du fortfarande uppmanas att ange ditt lösenord när du sparar inställningarna gör du på följande sätt:
  1. Öppna gatewayens webbaserade verktyg genom att gå till http://192.168.1.1 eller gatewayens IP-adress. Ange det förvalda användarnamnet och lösenordet **admin** och klicka på fliken **Administrations** => **Management** (Administration => Hantering).
  2. Ange ett annat lösenord i fältet Gateway Password (Gateway-lösenord) och bekräfta lösenordet genom att ange samma lösenord i det andra fältet.
  3. Klicka på **Save Settings** (Spara inställningar).

*10. **Jag är en PPPoE-användare och behöver ta bort proxy-inställningarna eller dialogrutan för uppringning.***

Om du använder proxy-inställningar måste du avaktivera dem i datorn. Eftersom gatewayen fungerar som gateway för Internet-anslutningen behövs inga proxy-inställningar för datorn för att du ska få åtkomst. Följ dessa anvisningar när du vill kontrollera att du inte använder några proxy-inställningar och att den webbläsare du använder är inställd för direkt anslutning till nätverket.

- För Microsoft Internet Explorer 5.0 eller senare:
  1. Klicka på **Start**, **Inställningar** och **Kontrollpanelen**. Dubbelklicka på Internet-alternativ.
  2. Klicka på fliken **Anslutningar**.
  3. Klicka på knappen **LAN-inställningar** och avmarkera allt som är markerat.
  4. Klicka på **OK** när du vill gå tillbaka till föregående skärm.
  5. Markera alternativet **Ring aldrig upp någon anslutning**. Eventuella uppmaningar att ringa upp tas nu bort för PPPoE-användare.

- För Netscape 6 eller senare:
  1. Starta **Netscape Navigator** och klicka på **Redigera**, **Inställningar**, **Avancerat** och **Proxy**.
  2. Kontrollera att Direkt anslutning till Internet är markerat på den här skärmen.
  3. Avsluta genom att stänga alla fönster.

11. Jag vill börja från början och måste därför återställa gatewayens fabriksinställningar.

Håll in knappen **Reset** (Återställ) i 10 sekunder och släpp den sedan. Internet-inställningar, lösenord, vidarebefordran och andra inställningar för gatewayen återställs då till fabriksinställningarna. Med andra ord så återgår gatewayen till sin fabrikskonfiguration.

12. Jag behöver uppgradera den fasta programvaran.

Om du vill uppgradera den fasta programvaran med de senaste funktionerna går du till Linksys internationella webbplats och laddar ned den senaste fasta programvaran på www.linksys.com/international.

- Gör så här:
  1. Gå till Linksys internationella webbplats på http://www.linksys.com/international och välj aktuellt område eller land.
  2. Klicka på fliken **Products** (Produkter) och välj aktuell gateway.
  3. På gatewayens webbsidan klickar du på **Firmware** (Fast programvara) och laddar sedan ned den senaste fasta programvaran för gatewayen.
  4. När du vill uppgradera den fasta programvaran följer du anvisningarna i avsnittet Administration i "Kapitel 5: Konfigurera Wireless-G-ADSL-gatewayen för hemmet".

13. Uppgraderingen av den fasta programvaran misslyckades och/eller strömlysdioden blinkar.

Uppgraderingen kan misslyckas av olika skäl. Följ anvisningarna nedan när du vill uppgradera den fasta programvaran och/eller få strömlysdioden att sluta blinka:

- Om uppgraderingen av den fasta programvaran misslyckas använder du TFTP-programmet (som du laddade ned tillsammans med den fasta programvaran). Öppna den pdf-fil som du laddade ned tillsammans med den fasta programvaran, starta TFTP-programmet och följ anvisningarna i pdf-filen.
- Ange en statisk IP-adress för datorn. Se avsnittet "Problem 1: Jag behöver ange en statisk IP-adress". Använd följande IP-adressinställningar för den dator du använder:
  IP Address (IP-adress): 192.168.1.50
  Subnet Mask (Nätmask): 255.255.255.0
  Gateway: 192.168.1.1
- Utför uppgraderingen med hjälp av TFTP-programmet eller på fliken Administration i gatewayens webbaserade verktyg.

14. Min DSL-tjänsts PPPoE-anslutning kopplas alltid ned.

En PPPoE-anslutning är i själva verket inte en anslutning som alltid är uppkopplad. Leverantören av DSL-anslutningen kan koppla ned tjänsten efter en viss period av inaktivitet, på samma sätt som en uppringd anslutning till Internet.

- Det finns en konfigureringsalternativ för att behålla anslutningen. Det fungerar inte alltid, så du kan ändå behöva återupprätta anslutningen med jämna mellanrum.
  1. När du vill ansluta till gatewayen öppnar du webbläsaren och anger http://192.168.1.1 eller gatewayens IP-adress.
  2. Ange användarnamn och lösenord om du tillfrågas. (Förvalt användarnamn och lösenord är admin.)
  3. På skärmen Setup (Konfigurera) markerar du alternativet **Keep Alive** (Behåll anslutning) och anger 20 sekunder för alternativet Redial Period (Återuppringningsperiod).
  4. Klicka på **Save Settings** (Spara inställningar). Klicka på fliken **Status** och klicka på knappen **Connect** (Anslut).
  5. Som inloggningsstatus kan Connecting (Ansluter) visas. Tryck på F5 key så att visningen uppdateras, tills inloggningsstatus Connected (Ansluten) visas.
  6. Klicka på **Save Settings** (Spara inställningar) när du vill fortsätta.
- Om anslutningen förloras på nytt återupprättar du den genom att följa stegen 1–6 .

15. Jag får inte åtkomst till e-post, webben eller VPN-nätverket, eller så erhåller jag felaktiga data från Internet.

MTU-inställningen (Maximum Transmission Unit) kan behöva ändras. Som standard ställs MTU in automatiskt.

- Om du får problem kan du göra på följande sätt:
  1. När du vill ansluta till gatewayen öppnar du webbläsaren och anger http://192.168.1.1 eller gatewayens IP-adress.
  2. Ange användarnamn och lösenord om du tillfrågas. (Förvalt användarnamn och lösenord är admin.)
  3. Leta rätt på MTU-alternativet och välj **Manual** (Manuell). I fältet Size (Storlek) anger du 1492.
  4. Klicka på **Save Settings** (Spara inställningar) när du vill fortsätta.
- Om problemen kvarstår ändrar du fältet Size (Storlek) till olika värden. Pröva följande värden i tur och ordning tills problemet är avhjälpt:
  1462
  1400
  1362
  1300

16. Strömlysdioden blinkar kontinuerligt.

Strömlysdioden tänds när enheten slås på. Under tiden startas enheten och funktionen kontrolleras. När kontrollproceduren är slutförd lyser lysdioden med ett fast sken, vilket innebär att systemet fungerar som det ska. Om lysdioden fortsätter blinka fungerar inte enheten på rätt sätt. Pröva i så fall att ange en statisk IP-adress för datorn och uppgradera den fasta programvaran. Pröva att använda följande inställningar: IP Address (IP-adress): 192.168.1.50 och Subnet Mask (Nätmask): 255.255.255.0.

17. När jag anger en URL-adress eller IP-adress får jag ett meddelande om överskriden tidsgräns och en uppmaning att försöka igen.

- Kontrollera att de andra datorerna fungerar. Om de gör det ser du till att datorns IP-inställningar är korrekta (IP-adress, nätmask, standard-gateway och DNS). Starta om den dator som du har problem med.

- Om datorerna är rätt konfigurerade men ändå inte fungerar kontrollerar du gatewayen. Kontrollera att den är ansluten och påslagen. Anslut till den och kontrollera dess inställningar. (Om du inte kan ansluta till den kontrollerar du nätverks- och strömanslutningarna.)
- Om gatewayen är rätt konfigurerad kontrollerar du att Internet-anslutningen (DSL/kabelmodem osv.) fungerar korrekt. Du kan avlägsna gatewayen om du vill kontrollera en direkt anslutning.
- Konfigurera TCP/IP-inställningarna manuellt med en DNS-adress som tillhandahålls av Internet-leverantören.
- Se till att webbläsaren är inställd för direkt anslutning och att uppringning är avaktiverad. I Internet Explorer klickar du på **Verktyg**, **Internet-alternativ** och väljer sedan fliken **Anslutningar**. Kontrollera att alternativet **Ring aldrig upp någon anslutning** inte är markerat i Internet Explorer. I Netscape Navigator klickar du på **Redigera**, **Inställningar**, **Avancerat** och **Proxy**. Kontrollera att Netscape Navigator är inställd för **Direkt anslutning till Internet**.

18. Jag försöker få åtkomst till gatewayens webbaserade verktyg men inloggningsskärmen visas inte. I stället visas meddelandet "404 Forbidden".

Om du använder Windows Explorer gör du på följande sätt tills inloggningsskärmen för det webbaserade verktyget visas (för Netscape Navigator fordras liknande åtgärder):

1. Klicka på **Arkiv**. Kontrollera att *Arbeta offline* INTE är markerat.
2. Tryck på **CTRL + F5**. Det är en hård uppdatering som tvingar Windows Explorer att läsa in nya webbsidor, inte cachade sådana.

- Klicka på **Verktyg**. Klicka på **Internet-alternativ**. Klicka på fliken **Säkerhet**. Klicka på knappen **Standardnivå**. Kontrollera att säkerhetsnivån är Normal eller lägre. Klicka på **OK**.

Vanliga frågor

Vilket är det högsta antal IP-adresser som kan användas med gatewayen?

Gatewayen kan användas med upp till 253 IP-adresser.

Kan IPSec-genomströmning användas med gatewayen?

Ja, det är en inbyggd funktion som är aktiverad som standard.

Var är gatewayen installerad i nätverket?

I en typisk miljö är gatewayen installerad mellan ADSL-uttaget och nätverket.

Kan IPX eller AppleTalk användas med gatewayen?

Nej. TCP/IP är den enda protokollstandarden för Internet och har blivit den globala standarden för kommunikation. IPX, som är ett NetWare-kommunikationsprotokoll som endast används för att dirigera meddelanden från en nod till en annan, och AppleTalk, som är ett kommunikationsprotokoll som används i Apple- och Macintosh-nätverk, kan användas för anslutningar mellan nätverk, men dessa protokoll kan inte användas för anslutning från Internet till ett nätverk.

Har nätverksanslutningen för gatewayen stöd för 100 Mbit/s Ethernet?
Gatewayen har stöd för 100 Mbit/s via den autoavkännande Fast Ethernet 10/100-switchen på gatewayens nätverkssida.

Vad är NAT (Network Address Translation) och vad används det till?
NAT (Network Address Translation) används för att översätta flera IP-adresser i ett privat nätverk till en allmän adress som skickas ut till Internet. Det ger en högre säkerhet eftersom adressen för en dator som är ansluten till det privata nätverket aldrig överförs till Internet. Dessutom ger NAT möjlighet att använda gatewayen med prisvärda Internet-konton när endast en TCP/IP-adress tillhandahålls av Internet-leverantören. Användaren kan ha många privata adresser bakom den här enda adressen som tillhandahålls av Internet-leverantören.

Kan gatewayen användas med några andra operativsystem än Windows 98SE, Windows Millennium, Windows 2000 och Windows XP?
Ja, men Linksys tillhandahåller för närvarande inte teknisk support för installation, konfigurering och felsökning för andra operativsystem än Windows.

Går det att skicka filer via ICQ med gatewayen?
Ja, med följande inställningsändring: Klicka på ICQ-menyn -> preference (inställningar) -> fliken connections (anslutningar) -> och markera I am behind a firewall or proxy (Jag befinner mig bakom en brandvägg eller proxy). Ange sedan brandväggens tidsgräns till 80 sekunder i brandväggsinställningarna. En Internet-användare kan sedan skicka filer till en användare bakom gatewayen.

Jag konfigurerar en Unreal Tournament-server, men andra i nätverket kan inte ansluta sig. Vad behöver jag göra?
Om du kör en särskild Unreal Tournament-server behöver du skapa en statisk IP-adress för varje dator i nätverket och vidarebefordra portarna 7777, 7778, 7779, 7780, 7781 och 27900 till serverns IP-adress. Du kan även använda ett intervall för vidarebefordran av port om 7777–27900. Om du vill använda UT Server Admin vidarebefordrar du en annan port. (Port 8080 fungerar i allmänhet bra men används för fjärradministrering. Du kan behöva avaktivera det här alternativet.) I avsnittet [UWeb.WebServer] i filen server.ini anger du ListenPort till 8080 (så att den stämmer med den avbildade porten ovan) och ServerName till den IP-adress som tilldelats gatewayen från Internet-leverantören.

Kan flera spelare i nätverket få åtkomst till en spelserver och spela samtidigt med endast en publik IP-adress?
Det beror på vilket nätverksspel eller vilken typ av spelserver det är fråga om. I till exempel Unreal Tournament kan flera logga in med en publik IP-adress.

Hur får jag Half-Life: Team Fortress att fungera med gatewayen?
Den förvalda klientporten för Half-Life är 27005. Datorerna i nätverket behöver få "+clientport 2700x" tillagt på HL-genvägens kommandorad. x är 6, 7, 8 och uppåt. På så sätt kan flera datorer ansluta till samma server. Ett problem: I version 1.0.1.6 kan inte flera datorer med samma CD-nyckel ansluta samtidigt, även om de tillhör samma nätverk (det här är inte ett problem med 1.0.1.3). När det gäller att fungera som värd för spel behöver inte HL-servern vara placerad i DMZ-zonen. Vidarebefordra bara port 27015 till den lokala IP-adressen för serverdatorn.

Webbsidor slutar svara, nedladdningar blir felaktiga eller inget annat än skräptecken visas på skärmen. Vad behöver jag göra?
Tvinga Ethernet-adaptern till 10 Mbit/s eller halv duplex och stäng av Ethernet-adapterns funktion för automatisk förhandling som en tillfällig åtgärd. (Se efter på fliken Avancerade egenskaper under Nätverk på Kontrollpanelen för Ethernet-adaptern.) Kontrollera att proxy-inställningen är avaktiverad i webbläsaren. Gå till vår webbplats på www.linksys.com/international om du behöver mer information.

Vad kan jag göra om allt annat misslyckas vid installationen?
Återställ gatewayen genom att hålla in återställningsknappen tills strömlysdioden tänds helt och släcks. Återställ DSL-modemet genom att stänga av och sätta på det igen. Hämta och installera den senaste fasta programvaran som finns på Linksys internationella webbplats, www.linksys.com/international.

Hur blir jag underrättad om nya uppgraderingar av den fasta programvaran för gatewayen?
Alla uppgraderingar av Linksys fasta programvara annonseras på Linksys internationella webbplats på www.linksys.com/international, där de kan laddas ned utan kostnad. När du vill uppgradera gatewayens fasta programvara använder du fliken Administration i gatewayens webbaserade verktyg. Om gatewayens Internet-anslutning fungerar bra finns det inget behov av att ladda ned en senare version av den fasta programvaran, såvida inte den versionen innehåller nya funktioner som du vill använda.

Fungerar gatewayen i Macintosh-miljö?
Ja, men gatewayens konfigureringssidor kan endast nås via Internet Explorer 4.0 eller Netscape Navigator 4.0 eller senare för Macintosh.

Jag kan inte visa gatewayens webbkonfigurationsskärm. Vad kan jag göra?
Du kan behöva avlägsna webbläsarens proxy-inställningar, t ex Netscape Navigator eller Internet Explorer. Se efter i webbläsarens dokumentation att den är inställd för direkt anslutning och att uppringning är avaktiverad. I Internet Explorer klickar du på Verktyg, Internet-alternativ och väljer sedan fliken Anslutningar. Kontrollera att alternativet Ring aldrig upp någon anslutning inte är markerat i Internet Explorer. I Netscape Navigator klickar du på Redigera, Inställningar, Avancerat och Proxy. Kontrollera att Netscape Navigator är inställd för Direkt anslutning till Internet.

Vad är en DMZ-värd?
Med DMZ (Demilitarized Zone) blir en IP-adress (dator) synlig mot Internet. För vissa program fordras att flera TCP/IP-portar är öppna. Du bör ange en statisk IP-adress för datorn om du vill använda den som en DMZ-värd. Information om hur du tar reda på IP-adressen i nätverket finns i "Bilaga C: Hitta MAC- och IP-adressen för Ethernet-adaptern".

Om jag använder en DMZ-värd, delar den då publik IP-adress med gatewayen?
Nej.

Passeras PPTP-paket genom eller dirigeras PPTP-sessioner aktivt med gatewayen?
PPTP-paket tillåts passera genom gatewayen.
Är gatewayen kompatibel med flera plattformar?
Alla plattformar där Ethernet och TCP/IP används är kompatibla med gatewayen.

Hur många portar kan vidarebefordras samtidigt?
Teoretiskt kan 520 sessioner upprättas samtidigt med gatewayen, men du kan endast vidarebefordra tio portintervall.

Vilka är de avancerade funktionerna hos gatewayen?
Gatewayens avancerade funktioner innefattar avancerade trådlösa inställningar, filter, vidarebefordrad av portar, dirigering och DDNS.

Vilket är det maximala antalet VPN-sessioner som tillåts för gatewayen?
Det maximala antalet beror på flera faktorer. Minst en IPSec-session kan användas via gatewayen. Samtidiga IPSec-sessioner kan dock vara möjliga, beroende på VPN-nätverkets utformning.

Hur kan jag kontrollera om jag har statiska IP-adresser eller DHCP-IP-adresser?
Kontakta din Internet-leverantör för den här informationen.

Hur får jag mIRC att fungera med gatewayen?
På fliken Port Forwarding (Vidarebefordran av portar) anger du vidarebefordran av port 113 för den dator där du använder mIRC.

Kan gatewayen fungera som en DHCP-server?
Ja. Gatewayen har inbyggd programvara för DHCP-server.

Kan jag köra ett program från en fjärransluten dator över det trådlösa nätverket?
Det beror på om programmet är avsett att köras över ett nätverk eller inte. Information om det kan köras över ett nätverk finns i programmets dokumentation.

Vad är standarden IEEE 802.11g?

Det är en av IEEE-standarderna för trådlösa nätverk. Med standarden 802.11g kan trådlös nätverkskommunikation upprättas mellan enheter från olika tillverkare, under förutsättning att enheterna följer 802.11g-standarden. I standarden 802.11g fastslås en maximal dataöverföringshastighet på 54 Mbit/s och en driftsfrekvens på 2,4 GHz.

Vilka IEEE 802.11b- och 802.11g-funktioner kan användas?

Produkten kan hantera följande IEEE 802.11b- och IEEE 802.11g-funktioner:

- Tillkännagivandeprotokollet CSMA/CA plus
- Flerkanals-roaming
- Automatiskt hastighetsval
- RTS/CTS
- Fragmentering
- Energisparfunktioner

Stöd finns även för OFDM-teknik för 802.11g-nätverk.

Vad är ad-hoc-läge?

När ett trådlöst nätverk är inställt på ad-hoc-läge är de trådlöst anslutna datorerna konfigurerade för att kommunicera direkt med varandra, utan användning av en accesspunkt.

Vad är infrastrukturläge?

När ett trådlöst nätverk är inställt på infrastrukturläge är det trådlösa nätverket konfigurerat för att kommunicera med ett nätverk via en trådlös accesspunkt.

Vad är roaming?

Roaming innebär att en användare av en bärbar dator kan kommunicera fortlöpande och samtidigt röra sig fritt över ett område som är större än det som täcks av en enda accesspunkt. Innan roaming-funktionen kan användas måste datorn fastställa att den har samma kanalnummer som accesspunkten för avsett täckningsområde.

Om verklig sömlös anslutning ska erhållas måste det trådlösa nätverket innehålla ett antal olika funktioner. Varje nod och accesspunkt måste till exempel alltid tillkännage mottagandet av varje meddelande. Varje nod måste upprätthålla kontakten med det trådlösa nätverket även när inga data överförs. För att dessa funktioner ska kunna uppnås samtidigt fordras en dynamisk RF-nätverksteknik som länkar accesspunkter och noder. I ett sådant system företar användarens slutnod en sökning efter den bästa möjliga åtkomsten till systemet. Först utvärderas sådana faktorer som signalstyrka och kvalitet samt den meddelandebelastning som för tillfället bärs av varje accesspunkt och avståndet för varje accesspunkt i förhållande till det trådanslutna stamnätet. Baserat på den informationen väljer sedan noden rätt accesspunkt och registrerar dess adress. Kommunikation mellan slutnoden och värddatorn kan därefter överföras upp och ned längs stamnätet.

När användaren förflyttar sig kontrollerar slutnodens RF-sändare regelbundet systemet för att fastställa om det har kontakt med den ursprungliga accesspunkten eller om det måste söka efter en ny. När noden inte längre erhåller tillkännagivande från den ursprungliga accesspunkten inleds en ny sökning. När en ny accesspunkt hittas omregistreras den och kommunikationsprocessen fortsätter.

Vad är ISM-bandet?

FCC och deras motsvarigheter utanför USA har öronmärkt bandbredd för olicensierad användning på ISM-bandet (Industrial, Scientific and Medical). Ett spektrum i området kring 2,4 GHz har gjorts tillgängligt över hela världen. Detta utgör ett verkligt revolutionerande tillfälle att placera bekväma trådlösa möjligheter med hög hastighet i händerna på användare över hela världen.

Vad är Spread Spectrum?

Spread Spectrum-tekniken är en frekvensteknik för bredbandsradio som har utvecklats av militären för användning i tillförlitliga, säkra och uppdragskritiska kommunikationssystem. Den är utformad för att offra bandbreddseffektivitet för tillförlitlighet, integritet och säkerhet. Med andra ord konsumeras mer bandbredd än vid smalbandsöverföring men förlusten uppvägs av att signalen är starkare och därmed enklare att upptäcka, under förutsättning att mottagaren känner till parametrarna för den Spread Spectrum-signal som sänds ut. Om en mottagare inte är inställd på rätt frekvens ser en Spread Spectrum-signal ut som bakgrundsbrus. Det finns två huvudalternativ, DSSS (Direct Sequence Spread Spectrum) och FHSS (Frequency Hopping Spread Spectrum).

Vad är DSSS? Vad är FHSS? Vad är skillnaden?

För FHSS (Frequency-Hopping Spread-Spectrum) används en smalbandsbärvåg som ändrar frekvens enligt ett mönster som är känt för både sändare och mottagare. Rätt synkroniserade blir nettoeffekten att en enda logisk kanal vidmakthålls. För en icke avsedd mottagare förefaller FHSS vara impulsbrus med kort varaktighet. Med DSSS (Direct-Sequence Spread-Spectrum) genereras ett redundant bitmönster för varje bit som ska överföras. Bitmönstret kallas för ett chip (eller chippningskod). Ju längre chip desto större sannolikhet för att ursprungliga data kan återställas. Även om en eller flera bitar i chipet skadas vid överföringen säkerställer statistiska tekniker i radion att ursprungliga data kan återställas utan att omsändning behövs. För en icke avsedd mottagare förefaller DSSS vara bredbandsbrus med låg signalstyrka och avvisas (ignoreras) av de flesta smalbandsmottagare.

Kan informationen fångas upp medan den färdas genom luften?

WLAN innefattar ett tvåfaldigt säkerhetsskydd. På maskinvarusidan finns, precis som för DSSS-teknik (Direct Sequence Spread Spectrum), en inbyggd säkerhetsfunktion i form av förvrängning. På programvarusidan innehåller WLAN en krypteringsfunktion (WEP) som ger förbättrad säkerhet och åtkomstkontroll.

Vad är WEP?

WEP är en förkortning av Wired Equivalent Privacy, en datasekretessmekanism baserad på en 64-bitars eller 128-bitars algoritm med delad nyckel, så som beskrivs i standarden IEEE 802.11.

Vad är en MAC-adress?

MAC-adressen (Media Access Control) är ett unikt nummer som tilldelas av tillverkaren till varje Ethernet-nätverksenhet, t ex nätverksadapter. Det här gör det möjligt att identifiera enheten på maskinvarunivå i nätverket. För alla praktiska ändamål är det här numret vanligen permanent. I motsats till IP-adresser, som kan ändras varje gång en dator loggas in till nätverket, förblir MAC-adressen för en enhet densamma, vilket gör den till en värdefull identifierare i nätverket.

Hur återställer jag gatewayen?

Tryck på knappen Reset (Återställ) på den bakre panelen i cirka tio sekunder. Gatewayen återställs då till sina standardinställningar.

Hur avhjälper jag problemet med signalförlust?

Det går inte att veta den exakta räckvidden för ett trådlöst nätverk utan att testa. Varje hinder som placeras mellan gatewayen och datorn medför en signalförlust. Blyat glas, metall, betonggolv, vatten och väggar hindrar signalen så att räckvidden minskar. Starta med gatewayen och den trädlösa datorn i samma rum och öka sedan avståndet stegvis så att du kan fastställa den maximala räckvidden i miljön.

Du kan även pröva att använda olika kanaler eftersom det kan eliminera störningar som påverkar endast en kanal.

Jag har utmärkt signalstyrka men jag kan inte hitta nätverket.

WEP är förmodligen aktiverat för gatewayen men inte för den trådlösa nätverksadaptern (eller vice versa). Kontrollera att samma WEP-nycklar och nivåer (64 eller 128) används för alla noder i det trådlösa nätverket.

Hur många kanaler/frekvenser är tillgängliga med gatewayen?

I Nordamerika finns elva kanaler tillgängliga, från 1 till 11. Det kan finnas ytterligare kanaler tillgängliga i andra områden, beroende på bestämmelser för området och/eller landet.

Om du har frågor som inte tas upp här kan du gå till Linksys internationella webbplats, www.linksys.com/international.

Bilaga B: Trådlös säkerhet

Linksys målsättning är att göra det så säkert och enkelt som möjligt att använda trådlösa nätverk. Den senaste generationen Linksys-produkter innehåller flera funktioner för nätverkssäkerhet, men det fordras vissa åtgärder från din sida för att implementera dem. Så håll följande i åtanke när du konfigurerar och använder ett trådlöst nätverk.

Säkerhetsåtgärder

Nedan visas en fullständig lista med de säkerhetsåtgärder som bör vidtas (minst steg 1 till 5 bör utföras):

1. Ändra standard-SSID.
2. Avaktivera SSID Broadcast.
3. Ändra standardlösenord för administratörskontot.
4. Aktivera MAC-adressfiltrering.
5. Ändra SSID med jämna mellanrum.
6. Använd den starkast möjliga krypteringsalgoritmen. Använd WPA om det är tillgängligt. Observera att det kan försämra nätverkets prestanda.
7. Ändra WEP-krypteringsnycklarna med jämna mellanrum.

Information om hur du implementerar de här säkerhetsfunktionerna finns i "Kapitel 6: Konfigurera Wireless-G ADSL-gateway för hemmet".



OBS! Vissa av de här säkerhetsfunktionerna är endast tillgängliga via nätverkets gateway, router eller accesspunkt. Läs dokumentationen för den gateway, router eller accesspunkt du använder om du behöver mer information.

Säkerhetshot mot trådlösa nätverk

Trådlösa nätverk är lätta att hitta. Hackare vet att för att ansluta till ett trådlöst nätverk lyssnar nätverksprodukterna först efter "signalmeddelanden". Meddelandena kan enkelt dekrypteras och innehåller mycket av nätverkets information, t ex nätverkets SSID (Service Set Identifier). Här är några åtgärder du kan vidta:

Ändra administratörslösenordet regelbundet. För varje trådlös nätverksenhet du använder bör du tänka på att nätverksinställningarna (SSID, WEP-nycklar osv.) lagras i den fasta programvaran. Nätverksadministratören är den enda person som kan ändra nätverksinställningarna. Om en hackare får tag i administratörslösenordet kan han också ändra inställningarna. Gör det därför svårare för en hackare att få tag i den informationen. Ändra administratörslösenordet regelbundet.

SSID: Det finns flera saker du bör tänka på när det gäller SSID:

1. Avaktivera Broadcast
2. Gör det unikt
3. Ändra det ofta

För de flesta trådlösa nätverksenheter har du möjlighet att sända ut SSID. Det alternativet kan vara bekvämare, eftersom det ger vem som helst möjlighet att logga in i det trådlösa nätverket. Det innefattar även hackare. Sänd därför inte ut SSID.

Trådlösa nätverksprodukter levereras med ett standard-SSID som konfigureras på fabriken. (För Linksys är standard-SSID "linksys".) Hackare känner till de här standardinställningarna och kan kontrollera om de används i nätverket. Ändra SSID till något unikt och inte något som går att koppla till företaget eller de nätverksprodukter som används.

Ändra SSID regelbundet så att eventuella hackare som fått åtkomst till det trådlösa nätverket måste börja om från början om de vill bryta sig in.

MAC-adresser. Aktivera MAC-adressfiltrering. Med hjälp av MAC-adressfiltrering kan du medge åtkomst till endast trådlösa noder med vissa MAC-adresser. Det gör det svårare för en hackare att få åtkomst till nätverket med en slumpartad MAC-adress.

WEP-kryptering. WEP (Wired Equivalent Privacy) ses ofta som en universallösning på alla säkerhetsproblem. Det är att överskatta möjligheterna med WEP. Du får endast tillräcklig säkerhet för att försvåra en hackares jobb.

Det finns flera sätt att maximera WEP:

1. Använd starkast möjliga krypteringsalgoritm.
2. Använd autentisering med delad nyckel
3. Ändra WEP-nyckel regelbundet



VIKTIGT! Glöm inte att samma krypteringsmetod och nyckel MÅSTE användas för varje enhet i det trådlösa nätverket, annars fungerar inte det trådlösa nätverket på rätt sätt.

WPA. WPA (Wi-Fi Protected Access) är den senaste och bästa standarden för trådlös säkerhet. Det finns två lägen: Pre-Shared Key (För-delad nyckel) och RADIUS. Med Pre-Shared Key (För-delad nyckel) kan du välja mellan två krypteringsmetoder: TKIP (Temporal Key Integrity Protocol), som innefattar en starkare krypteringsmetod och MIC (Message Integrity Code) som ett skydd mot hackare, samt AES (Advanced Encryption System), som innefattare en symmetrisk datakryptering med 128-bitarsblock. RADIUS (Remote Authentication Dial-In User Service) innefattar en RADIUS-server för autentisering och användning av dynamisk TKIP, AES eller WEP.

WPA med för-delad nyckel. Om du inte har någon RADIUS-server väljer du typ av algoritm, TKIP eller AES, anger ett lösenord i fältet Pre-Shared key (För-delad nyckel) om 8-64 tecken och anger en gruppförnyelseperiod mellan 0 och 99 999 sekunder, vilket anger hur ofta krypteringsnycklarna ska ändras för gatewayen eller enheten.

WPA med RADIUS. WPA som används tillsammans med en RADIUS-server. (Det bör endast användas om en RADIUS-server är ansluten till gatewayen eller annan enhet.) Välj först typ av WPA-algoritm, **TKIP** eller **AES.** Ange RADIUS-serverns IP-adress och portnummer tillsammans med en nyckel som delas mellan enheten och servern. Slutligen anger du en period för förnyelse av gruppnyckel, vilket anger hur ofta krypteringsnycklarna ska ändras för enheten.

RADIUS. WEP som används tillsammans med en RADIUS-server. (Det bör endast användas om en RADIUS-server är ansluten till gatewayen eller annan enhet.) Börja med att ange RADIUS-serverns IP-adress och portnummer tillsammans med en nyckel som delas mellan enheten och servern. Välj sedan en WEP-nyckel och en nivå för WEP-kryptering, och ange sedan en WEP-nyckel manuellt eller med hjälp av lösenord.

Implementering av kryptering kan ha en negativ inverkan på nätverkets prestanda, men om du överför känsliga data i nätverket bör du använda kryptering.

De här säkerhetsrekommendationerna bör bidra till sinnesfrid när du använder den mest flexibla och bekväma teknik som Linksys kan erbjuda.

Bilaga C: Hitta MAC-adress och IP-adress för Ethernet-adaptern

I det här avsnittet beskrivs hur du hittar MAC-adressen för datorns Ethernet-adapter, så att du kan använda gatewayens MAC-filtreringsfunktion. Du kan också hitta IP-adressen för datorns Ethernet-adapter. IP-adressen används för filtrering och vidarebefordran av gatewayen och/eller DMZ-funktioner. Följ anvisningarna i den här bilagan när du vill hitta adapterns MAC- eller IP-adress i Windows 98, Me, 2000 eller XP.

Anvisningar för Windows 98 och Me

1. Klicka på **Start** och **Kör**. I fältet *Öppna* skriver du **winipcfg**. Tryck på **Enter** eller klicka på **OK**.
2. När dialogrutan *IP Configuration (IP-konfiguration)* visas markerar du den Ethernet-adapter som du har anslutit till gatewayen via en CAT 5 Ethernet-nätverkskabel. Se figur C-1.
3. Skriv ned adapteradressen så som den visas på datorns skärm (se figur C-2). Det här är MAC-adressen till Ethernet-adaptern och visas i hexadecimalt format som en serie siffror och bokstäver.

   MAC-adressen/adapteradressen används för MAC-filtrering. I exemplet i figur D-2 visas Ethernet-adapterns MAC-adress som 00-00-00-00-00-00. På datorn visas något annat.

   I exemplet i figur C-2 visas Ethernet-adapterns IP-adress som 192.168.1.100. På datorn visas kanske något annat.



Obs! MAC-adressen kallas även adapteradress.

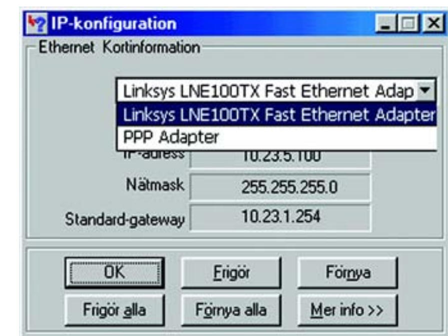


Bild C-1: Dialogruta för IP-konfiguration



Bild C-2: MAC-adress/adapteradress

Anvisningar för Windows 2000 och XP

1. Klicka på **Start** och **Kör.** I fältet *Öppna* skriver du **cmd.** Tryck på **Enter** eller klicka på **OK.**



Obs! MAC-adressen kallas även fysisk adress.

2. Vid kommandoprompten skriver du **ipconfig /all.** Tryck sedan på **Enter.**

3. Skriv ned den fysiska adressen så som den visas på skärmen (figur C-3). Det är MAC-adressen för Ethernet-adaptern. Den visas som en serie siffror och bokstäver.

   MAC-adressen/fysiska adressen används för MAC-filtrering. I exemplet i figur C-3 visas Ethernet-adapterns MAC-adress som 00-00-00-00-00-00. På datorn visas något annat.

   I exemplet i figur C-3 visas Ethernet-adapterns IP-adress som 192.168.1.100. På datorn visas kanske något annat.

```
C:\WINNT\system32\cmd.exe

C:\>ipconfig /all

Windows 2000 IP-konfiguration

        Värddatornamn . . . . . . . . . . :
        Primärt DNS-suffix  . . . . . . . :
        Nodtyp  . . . . . . . . . . . . . : Hybrid
        IP-routning aktiverat . . . . . . : Nej
        WINS-proxy aktiverat  . . . . . . : Nej

Kort: Ethernet  Local Area Connection:

        Anslutningsspecifika DNS-suffix . :
        Beskrivning . . . . . . . . . . . : Linksys LNE100X(v5) Fast Ethernet Adapter
        Fysisk adress . . . . . . . . . . : 00-00-00-00-00-00
        DHCP aktiverat  . . . . . . . . . : Ja
        Autoconfiguration är aktiverad  . : Ja
        IP-adress . . . . . . . . . . . . : 10.23.5.42
        Nätmask . . . . . . . . . . . . . : 255.255.255.0
        Standard-gateway  . . . . . . . . : 10.23.1.254
        DHCP-server . . . . . . . . . . . : 10.23.3.1
        DNS-servrar . . . . . . . . . . . : 10.23.3.3
        Primär WINS-server  . . . . . . . : 10.23.3.1
        Sekundär WINS-server  . . . . . . : 10.23.3.1
        Lånet erhölls . . . . . . . . . . : 08 April 2005 14:33:06
        Lånet upphör  . . . . . . . . . . : 11 April 2005 14:33:06

C:\>_
```

Bild C-3: MAC-adress/fysisk adress

Bilaga D: Uppgradera fast programvara

Uppgradera den fasta programvaran till gatewayen:

1. Ladda ned filen med uppdateringen av gatewayens fasta programvara från *www.linksys.com*.
2. Packa upp filen i datorn.
3. Öppna gatewayens webbaserade verktyg och klicka på fliken **Administration**.
4. Klicka på fliken **Firmware Upgrade** (Uppgradera fast programvara).
5. Klicka på knappen **Browse** (Bläddra), leta rätt på den uppackade filen och dubbelklicka på den.
6. Klicka på knappen **Upgrade** (Uppgradera) och följ anvisningarna på skärmen.



Bild D-1: Firmware Upgrade (Uppgradera fast programvara)

Bilaga E: Ordlista

802.11b - en standard för trådlösa nätverk med en maximal dataöverföringshastighet på 11 Mbit/s och en driftsfrekvens på 2,4 GHz.

802.11g - en standard för trådlösa nätverk med en maximal dataöverföringshastighet på 54 Mbit/s, en driftsfrekvens på 2,4 GHz och bakåtkompatibilitet med 802.11b-enheter.

Accesspunkt - en enhet som gör det möjligt för trådlösa datorer och andra enheter att kommunicera med ett trådanslutet nätverk. Används även för att utvidga räckvidden för ett trådlöst nätverk.

Ad-hoc - en grupp trådlösa enheter som kommunicerar direkt med varandra (serverlöst) utan att någon accesspunkt används.

AES (**A**dvanced **E**ncryption **S**tandard) - en säkerhetsmetod där symmetrisk datakryptering med 128-bitarsblock används.

Bandbredd - överföringskapacitet för en viss enhet eller nätverk.

Bit - en binär siffra.

"Boota" - starta en enhet så att körning av instruktioner inleds.

Brandvägg - ett uppsättning sammanhörande program som finns på ett nätverks gatewayserver och som skyddar resurserna i nätverket från användare i andra nätverk.

Bredband - en snabb Internet-anslutning med fast uppkoppling.

Brygga - en enhet för anslutning av flera nätverk.

Buffert - ett delat eller tilldelat minnesutrymme som används för att stödja och koordinera olika beräknings- och nätverksaktiviteter så att en inte uppehålls av en annan.

Byte - en dataenhet som i allmänhet är åtta bitar lång

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - en metod för dataöverföring som används för att förhindra datakollisioner.

CTS (**C**lear **T**o **S**end) - en signal som skickas från en trådlös enhet för att signalera att den är redo att ta emot data.

Databas - en samling data som organiseras så att dess innehåll enkelt kan hämtas, hanteras och uppdateras.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - möjliggör värdtjänster för en webbplats, FTP-server eller e-postserver med ett fast domännamn (t ex www.xyz.com) och en dynamisk IP-adress.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - ett nätverksprotokoll som används för att tilldela tillfälliga IP-adresser till nätverkets datorer genom att "leasa" en IP-adress till en användare under en begränsad tidsperiod, i stället för att tilldela permanenta IP-adresser.

DMZ (**D**emilitarized **Z**one) - tar bort routerns brandväggsskydd från en dator så att den "syns" från Internet.

DNS (**D**omain **N**ame **S**erver) - IP-adressen för Internet-leverantörens server, som översätter webbplatsernas namn till IP-adresser.

Domän - ett specifikt namn för ett nätverk med datorer.

DSL (**D**igital **S**ubscriber **L**ine) - en bredbandsanslutning med fast uppkoppling via traditionella telefonledningar.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - frekvensöverföring med ett redundant bitmönster som resulterar i mindre risk för informationsförlust vid överföringen.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - ett meddelande som inkluderas i datapaket i syfte att göra den trådlösa överföringen effektivare.

Dynamisk IP-adress - en tillfällig IP-adress som tilldelas från en DHCP-server.

EAP (**E**xtensible **A**uthentication **P**rotocol) - ett allmänt autentiseringsprotokoll som används för att kontrollera nätverksåtkomst. Många specifika autentiseringsmetoder fungerar inom det här ramverket.

EAP-PEAP (**E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol) - en ömsesidig autentiseringsmetod med en kombination av digitala certifikat och ett annat system, t ex lösenord.

EAP-TLS (**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity) - en ömsesidig autentiseringsmetod med digitala certifikat.

Ethernet - ett nätverksprotokoll som anger hur data placeras på och hämtas från ett gemensamt överföringsmedium.

Fast programvara - den programmeringskod som körs i en nätverksenhet.

Finger - ett program som används för att informera om vilket namn som är kopplat till en e-postadress.

Fragmentering - nedbrytning av ett paket i mindre enheter vid överföring via ett nätverksmedium där den ursprungliga paketstorleken inte kan användas.

FTP (**F**ile **T**ransfer **P**rotocol) - ett protokoll som används för att överföra filer i ett TCP/IP-nätverk.

Full Duplex - möjligheten för en nätverksenhet att ta emot och sända data samtidigt.

Gateway - en enhet som sammankopplar nätverk med andra, inkompatibla kommunikationsprotokoll.

Genomströmning - den mängd data som flyttas utan fel från en nod till en annan under en viss tidsperiod.

Halv Duplex - dataöverföring som kan ske i två riktningar över samma linje, men endast i en riktning åt gången.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - det kommunikationsprotokoll som används för att ansluta till servrar på World Wide Web.

Infrastruktur - ett trådlöst nätverk som är bryggkopplat till ett trådanslutet nätverk via en accesspunkt.

Internet-leverantör - ett företag som tillhandahåller åtkomst till Internet.

IP (**I**nternet **P**rotocol) - ett protokoll som används för att sända data över ett nätverk.

IP-adress - den adress som används för att identifiera en dator eller enhet i ett nätverk.

IPCONFIG - ett verktyg i Windows 2000 och XP för att visa IP-adressen för en viss nätverksenhet.

IPSec (**I**nternet **P**rotocol **S**ecurity) - ett VPN-protokoll som används för att implementera ett säkert utbyte av paket i IP-skiktet.

ISM-band - radiobandbredd som används i trådlösa överföringar.

Kabelmodem - en enhet för anslutning av en dator till kabeltelevisionsnätverket, som i sin tur ansluts till Internet.

Kryptering - kodning av data som överförs i ett nätverk.

Ladda ned - att hämta en fil via ett nätverk.

Ladda upp - att skicka en fil via ett nätverk.

LAN (**L**ocal **A**rea **N**etwork) - ett lokalt nätverk med datorer och annan nätverksutrustning.

LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol) - en ömsesidig autentiseringsmetod där ett system med användarnamn och lösenord används.

Lösenordsfras - används på samma sätt som ett lösenord. Med en lösenordsfras förenklas WEP-krypteringsprocessen genom att WEP-krypteringsnycklarna automatiskt genereras för produkterna från Linksys.

MAC-adress (**M**edia **A**ccess **C**ontrol) - den unika adress som en tillverkare tilldelar till varje nätverksenhet.

Maskinvara - de fysiska aspekterna av datorer, telekommunikation och andra informationstekniksenheter.

Mbit/s (**M**egabitar per **s**ekund) - en miljon bitar per sekund. en måttenhet för dataöverföring.

mIRC - ett IRC-program (Internet Relay Chat) som körs under Windows.

Multicasting - data som skickas till en grupp med mål samtidigt.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT-tekniken översätter IP-adresser i ett lokalt nätverk till en annan IP-adress för Internet.

Nätmask - en adresskod som avgör nätverkets storlek.

Nätverk - en serie datorer eller enheter anslutna i syfte att dela data, lagring och/eller överföring mellan användare.

Nätverkadapter - en enhet som lägger till nätverksfunktioner för datorn.

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) - det protokoll som används för att ansluta till Usenet-grupper på Internet.

Nod - en nätverkskoppling eller anslutningspunkt, i allmänhet en dator eller arbetsstation.

OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) - frekvensöverföring med separering av dataströmmen i ett antal dataströmmar med lägre hastighet, som sedan överförs parallellt i syfte att förhindra att information förloras vid överföringen.

Paket - en dataenhet som sänds över ett nätverk.

PEAP (**P**rotected **E**xtensible **A**uthentication **P**rotocol) - en ömsesidig autentiseringsmetod med en kombination av digitala certifikat och ett annat system, t ex lösenord.

Ping (**P**acket **IN**ternet **G**roper) - ett Internet-verktyg som används för att fastställa om en viss IP-adress är uppkopplad.

POP3 (**P**ost **O**ffice **P**rotocol 3) - en standardpostserver som ofta används på Internet.

Port - anslutningspunkten på en dator eller nätverksenhet dit kablar eller adaptrar ansluts.

Power over Ethernet (PoE) - en teknik med vilken både data och drivspänning kan levereras via en Ethernet-kabel.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - en typ av bredbandsanslutning med autentisering (användarnamn och lösenord) vid sidan av datatransport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - ett VPN-protokoll där PPP-protokollet (Point to Point Protocol) kan tunnlas genom ett IP-nätverk. Protokollet används också som en sorts bredbandsanslutning i Europa.

Preamble - del av en trådlös signal som används för att synkronisera nätverkstrafiken.

Programvara - Instruktioner till datorn. En serie instruktioner som utför en viss uppgift kallas för ett "program".

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - ett protokoll där en autentiseringsserver används för att kontrollera åtkomsten till nätverket.

RJ-45 (**R**egistered **J**ack-**45**) - ett Ethernet-kontaktdon för upp till åtta ledare.

Roaming - möjligheten att flytta en trådlös enhet från en accesspunkts räckvidd till en annan utan att förlora anslutningen.

Router - en nätverksenhet för sammankoppling av flera nätverk.

RTS (**R**equest **T**o **S**end) - en nätverksmetod för att koordinera stora paket genom RTS-tröskelinställningen.

Seriekoppling - en metod som används för att sammankoppla enheter i serie efter varandra.

Server - en dator vars funktion i ett nätverk är att tillhandahålla användaråtkomst till filer, utskrift, kommunikation och andra tjänster.

Signalintervall - data som överförs i det trådlösa nätverket så att synkronisering upprätthålls.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - standardprotokollet för e-post på Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - ett vanligt protokoll för övervakning och kontroll av ett nätverk.

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - marknadssegment för yrkesverksamma som arbetar hemma eller på små kontor.

SPI (**S**tateful **P**acket **I**nspection) Firewall - en teknik som inspekterar inkommande paket med data innan de får tillgång till nätverket.

Spritt spektrum - frekvensteknik för bredbandsradio som används för mer tillförlitlig och säker dataöverföring.

SSID (**S**ervice **S**et **ID**entifier) - det trådlösa nätverkets namn.

Stamnät - den del av ett nätverk som merparten av systemet är anslutet till och där den stora andelen data hanteras.

Standardgateway - en enhet som används för att vidarebefordra Internet-trafik från det lokala nätverket.

Statisk IP-adress - en fast adress som tilldelas en dator eller enhet som är ansluten till ett nätverk.

Statisk routning - vidarebefordran av data i ett nätverk via en fast sökväg.

Switch - 1. en dataswitch som ansluter datorenheter till värddatorer så att ett stort antal enheter kan dela på ett begränsat antal portar. 2. en enhet för att skapa, bryta eller ändra anslutningarna för en elektrisk krets.

TCP (**T**ransmission **C**ontrol **P**rotocol) - ett nätverksprotokoll för överföring av data som fordrar tillkännagivande från mottagaren av de data som sänds.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - en uppsättning instruktioner som används i datorer för att kommunicera via ett nätverk.

Telnet - ett användarkommando och TCP/IP-protokoll som används för åtkomst till fjärranslutna datorer.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - en version av TCP/IP FTP-protokollet som inte innehåller någon katalog eller lösenordsfunktion.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - ett trådlöst krypteringsprotokoll med dynamiska krypteringsnycklar för varje paket som överförs.

Topologi - nätverkets fysiska layout.

TX-hastighet - överföringshastighet.

UDP (**U**ser **D**atagram **P**rotocol) - ett nätverksprotokoll för överföring av data som inte fordrar tillkännagivande från mottagaren av de data som sänds.

Uppgradera - att ersätta befintlig programvara eller fast programvara med en nyare version.

URL (**U**niform **R**esource **L**ocator) - Adressen för en fil på Internet.

VPN (**V**irtual **P**rivate **N**etwork) - en säkerhetsåtgärd i syfte att skydda data när de lämnar ett nätverk och anländer till ett annat via Internet.

WAN (**W**ide **A**rea **N**etwork) - Internet.

Webbläsare - ett program som används för att ta del av och interagera med all information på World Wide Web.

WEP (**W**ired **E**quivalent **P**rivacy) - en metod för kryptering av nätverksdata som överförs i ett trådlöst nätverk, vilket ger högre säkerhet.

WINIPCFG - ett verktyg i Windows 98 och Me för att visa IP-adressen för en viss nätverksenhet.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - en grupp datorer och tillhörande enheter som kommunicerar trådlöst med varandra.

WPA (**Wi**-**Fi** **P**rotected **A**ccess) - ett trådlöst säkerhetsprotokoll med TKIP-kryptering (Temporal Key Integrity Protocol), som kan användas tillsammans med en RADIUS-server.

Bilaga F: Information om regler

Den här produkten uppfyller nödvändiga krav i EU-direktivet 1999/5/EC och gäller för alla EU-länder (det kan finnas vissa begränsningar).

Kompatibilitetsinformation för trådlösa produkter med hastigheten 2,4-GHz som gäller för EU och andra länder följer EU-direktivet 1999/5/EC (R&TTE-direktivet)

Deklaration om överensstämmelse med avseende på EU-direktivet 1995/5/EC (R&TTE-direktivet)

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

OBS! Om du behöver teknisk dokumentation kan du läsa avsnittet "Så här får du åtkomst till tekniska dokument på www.linksys.com/international".

Följande standarder användes vid bedömning av produkten mot kraven i direktivet 1999/5/EC:

- Radio: EN 300 328
- EMC: EN 301 489-1, EN 301 489-17
- Säkerhet: EN 60950

CE-märkning

För produkterna Linksys Wireless-B och Wireless-G har följande CE-märkning, meddelat höljenummer (i tillämpliga fall) och klass 2-identifierare lagts till för apparaturen.



Se efter på produktens CE-etikett vilket meddelat hölje som använts vid utvärderingen.

Nationella begränsningar

Den här produkten får användas i alla EU-länder (och andra länder som följer EU-direktivet 1999/5/EC) utan andra begränsningar än de som omnämns för vissa länder nedan:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

Belgien

Det belgiska institutet för postala tjänster och telekommunikation (BIPT) måste underrättas om varje trådlös länk som installeras utomhus med en räckvidd som överstiger 300 meter. Besök http://www.bipt.be om du vill få mer information.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Frankrike

Om produkten används utomhus är uteffekten begränsad i vissa delar av bandet. Se efter i tabell 1 eller besök http://www.art-telecom.fr/ om du vill få mer information.

Dans la cas d'une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous à la table 1 ou visitez http://www.art-telecom.fr/ pour de plus amples détails.

Tabell 1: Tillämpliga effektnivåer i Frankrike

Plats	Frekvensomfång (MHz)	Effekt (EIRP)
Inomhus (inga begränsningar)	2400-2483,5	100 mW (20 dBm)
Utomhus	2400-2454 2454-2483,5	100 mW (20 dBm) 10 mW (10 dBm)

Italien

Den här produkten uppfyller kraven för nationellt radiogränssnitt och tabellen för nationell frekvensallokering för Italien. Såvida inte den trådlösa nätverksprodukten med hastigheten 2,4 GHz används inom ägarens egendom fordras en allmän behörighet. Besök http://www.comunicazioni.it/it/ om du vill få mer information.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Begränsningar för användning av produkten

Produkten är endast avsedd för inomhusbruk. Utomhusbruk rekommenderas inte.

Produkten är avsedd för användning med den medföljande inbyggda eller externa där för avsedda antennen. Användning av annan antenn från annan tillverkare rekommenderas inte och stöds inte av Linksys.

Enhetens uteffekt

Det kan vara nödvändigt att ändra enhetens uteffekt för att den ska överensstämma med det aktuella landets föreskrifter. Gå vidare till lämpligt avsnitt för enheten.

OBS! Inställningen för uteffekt är inte tillgänglig för alla trådlösa produkter. Om du vill få mer information kan du läsa dokumentationen på produktens cd-skiva eller besöka http://www.linksys.com/international.

Trådlösa nätverksadaptrar

Trådlösa nätverksadaptrar har uteffekten inställd på 100 % som standard. Maximal uteffekt för varje adapter överstiger inte 20 dBm (100 mW), i allmänhet är den 18 dBm (64 mW) eller lägre. Om du behöver ändra den trådlösa nätverksadapterns uteffekt följer du anvisningarna för respektive version av operativsystemet Windows:

Windows XP

1. Dubbelklicka på ikonen **Trådlöst** i skrivbordets systemfält.
2. Öppna fönstret *Trådlös nätverksanslutning*.
3. Klicka på **Egenskaper.**
4. Välj fliken **Allmänt** och klicka på knappen **Konfigurera.**
5. I fönstret *Egenskaper* klickar du på fliken **Avancerat.**
6. Välj **Power Output** (Uteffekt).
7. På menyn till höger väljer du den trådlösa nätverksadapterns uteffekt i procent.

Windows 2000

1. Öppna **Kontrollpanelen.**
2. Dubbelklicka på **Nätverks- och fjärranslutningar.**
3. Välj den aktuella trådlösa anslutningen och välj sedan **Egenskaper.**
4. I dialogrutan *Egenskaper* klickar du på knappen **Konfigurera.**
5. Klicka på fliken **Avancerat** och välj **Power Output** (Uteffekt).
6. På menyn till höger väljer du den trådlösa nätverksadapterns uteffekt.

Om du använder Windows Millennium eller 98 kan du läsa i Windows-hjälpen hur du får åtkomst till de avancerade inställningarna för ett nätverksadaptrar.

Trådlösa accesspunkter, routrar och andra trådlösa produkter

Om du har en trådlös accesspunkt, router eller annan trådlös produkt, använder du det webbaserade verktyget när du vill konfigurera inställningen för uteffekt. (Läs dokumentationen till produkten om du vill få mer information).

Tekniska dokument för www.linksys.com/international

Följ anvisningarna nedan om du vill få åtkomst till tekniska dokument:

1. Besök http://www.linksys.com/international.
2. Klicka på det område där du befinner dig.
3. Klicka på namnet för det land där du befinner dig.
4. Klicka på **Products (Produkter)**.
5. Klicka på aktuell produktkategori.
6. Välj en produkt.
7. Klicka på den typ av dokumentation du vill läsa. Dokumentet öppnas automatiskt i PDF-format.

> OBS! Om du har frågor rörande dessa produkters kompatibilitet eller om du inte kan hitta den information du söker efter kontaktar du närmaste försäljningskontor. Besök http://www.linksys.com/international om du vill få mer information.

SÄKERHET

Varning! Minska brandrisken genom att endast använda telekabel 26 AWG eller grövre.

Använd inte produkten i närheten av vatten, exempelvis i en fuktig källare eller nära en simbassäng.

Undvik att använda produkten vid åskväder.

Bilaga G: Garantiinformation

Linksys garanterar att Linksys-produkten är felfri under en period av tre år ("garantiperioden") vad avser material och utförande vid normal användning. Linksys totala ansvar är att reparera eller ersätta produkten eller återbetala ditt inköpspris, minus eventuella rabatter. Denna begränsade garanti gäller endast den ursprungliga kunden.

Om produkten visar sig vara defekt under garantiperioden ringer du Linksys tekniska support och får ett returnummer, om det behövs. SE TILL ATT DU HAR INKÖPSKVITTOT TILL HANDS NÄR DU RINGER. Om du ombeds returnera produkten skriver du returnumret på paketets utsida och skickar med en kopia av originalkvittot. RETURER BEHANDLAS INTE UTAN KVITTO. Du ansvarar för att produkterna skickas till Linksys. Linksys betalar endast för ytpost via UPS från Linksys tillbaka till dig. Kunder utanför USA och Kanada ansvarar för alla leverans- och hanteringskostnader.

ALLA UNDERFÖRSTÅDDA GARANTIER OCH VILLKOR AVSEENDE PRODUKTENS ALLMÄNNA LÄMPLIGHET OCH/ELLER LÄMPLIGHET FÖR ETT SÄRKSILT ÄNDAMÅL ÄR BEGRÄNSADE TILL GARANTIPERIODENS VARAKTIGHET. ALLA ANDRA UTTRYCKLIGA ELLER UNDERFÖRSTÅDDA VILLKOR, FRAMSTÄLLNINGAR OCH GARANTIER, INKLUSIVE UNDERFÖRSTÅDDA GARANTIER FÖR INTRÅNG I UPPHOVSRÄTTEN, FRISKRIVS. Eftersom varaktigheten för begränsningar av underförstådda garantier inte är giltig i vissa länder, är det möjligt att ovanstående friskrivning och ansvarsbegränsning inte är tillämplig i ditt fall. Garantin ger dig särskilda rättigheter. Du kan även ha andra rättigheter som kan variera från land till land.

Garantin gäller inte om produkten (a) har ändrats, förutom av Linksys, (b) inte har installerats, körts, reparerats eller underhållits i enlighet med instruktionerna från Linksys eller (c) har utsatts för onormala fysiska eller elektriska påkänningar, felaktig användning, vårdslöshet eller olycka. Linksys arbetar ständigt med att utveckla nya tekniker för skydd mot intrång i nätverk och kan därför inte garantera att produkten är osårbar vid intrång eller attacker.

MED UNDANTAG AV VAD SOM GÄLLER FÖR AKTUELLA LAGAR, ANSVARAR LINKSYS INTE FÖR FÖRLORADE DATA ELLER UTEBLIVNA FÖRTJÄNSTER, INDIREKTA, SKADESTÅNDSFÖRPLIKTANDE, TILLFÄLLIGA ELLER SÄRSKILDA FÖLJDSKADOR ELLER ANDRA SKADOR, OAVSETT TEORETISKT ANSVAR (INKLUSIVE FÖRSUMLIGHET) SOM ÄR RELATERADE TILL ANVÄNDNINGEN ELLER OFÖRMÅGAN ATT ANVÄNDA PRODUKTEN (INKLUSIVE EVENTUELL PROGRAMVARA), ÄVEN OM LINKSYS HAR UPPMÄRKSAMMATS PÅ RISKEN FÖR SÅDANA SKADOR. UNDER ALLA OMSTÄNDIGHETER BEGRÄNSAR SIG LINKSYS ANSVAR TILL DET BELOPP SOM DU HAR BETALAT FÖR PRODUKTEN. Ovannämnda begränsningar gäller även om garanti eller kompensation inte sker enligt avsett syfte. Vissa länder tillåter inte friskrivningar enligt ovan. Därför kanske inte ovanstående begränsningar gäller dig.

Garantin är giltig och kan endast behandlas i inköpslandet.

Frågor hänvisas till: Linksys, P.O. Box 18558, Irvine, CA 92623.

Bilaga H: Specifikationer

Modellnummer	WAG354G
Standarder	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, G.992.1 (G.dmt), G.992.2 (G.lite), G.992.3, G.992.5, T1.413i2
Portar	Power, ADSL, Ethernet (1-4)
Knapp	Reset
Kabeltyp	KAT 5 UTP
Lysdioder	Power, Wireless, Ethernet (1-4), DSL, Internet
Överföringseffekt	18 dBm
Kanaler	13 (stora delar av Europa)
UPnP-funktion/cert.	Hanterar
Säkerhetsfunktioner	Lösenordsskyddad konfiguration för Internet-åtkomst PAP- och CHAP-autentisering DoS-skydd (Denial of Service) URL-filtrering och blockering baserat på nyckelord, Java, ActiveX, Proxy och cookiefiler ToD-filter (begränsar åtkomst till vissa tider) VPN-genomströmning med IPSec-, PPTP- och L2TP-protokollen WEP med 64 eller 128 bitar med generering av WEP-nyckel med lösenord Avaktiverad SSID Broadcast Begränsad åtkomst via MAC- och IP-adresser
WEP-nyckelbitar	64, 128

Dimensioner	140 mm x 140 mm x 27 mm
Vikt	0,3 kg
Strömförsörjning	12 V DC 1 A
Certifieringar	CE
Driftstemperatur	0º~40º C
Förvaringstemperatur	-20º~70º C
Luftfuktighet vid drift	10~85 % icke-kondenserande
Luftfuktighet vid förvaring	5~90 % icke-kondenserande

Bilaga I: Kontaktinformation

Behöver du kontakta Linksys?
Om du vill ha information om de senaste produkterna och uppdateringarna till dina befintliga produkter kan du besöka oss online på:
http://www.linksys.com/international

Om du har problem med någon Linksys-produkt kan du skicka e-post till oss på:

I Europa	E-postadress
Belgien	support.be@linksys.com
Danmark	support.dk@linksys.com
Frankrike	support.fr@linksys.com
Italien	support.it@linksys.com
Nederländerna	support.nl@linksys.com
Norge	support.no@linksys.com
Österrike	support.at@linksys.com
Portugal	support.pt@linksys.com
Schweiz	support.ch@linksys.com
Spanien	support.es@linksys.com
Storbritannien och Irland	support.uk@linksys.com
Sverige	support.se@linksys.com
Tyskland	support.de@linksys.com

Utanför Europa	E-postadress
Latinamerika	support.la@linksys.com
USA och Kanada	support@linksys.com





DECLARATION OF CONFORMITY

With regard to the R&TTE Directive 1999/5/EC

According to EN 45014

Cisco-Linksys LLC
121 Theory Drive
Irvine, CA 92617
USA

Declares under our sole responsibility that the product,

Linksys WAG354G / Wireless-G ADSL Home Gateway (Annex A)

Variants: WAG354G –XX where XX may stand for BG, BT, DE,FR, EU, E1, SE or UK (where applicable)

Fulfills the essential requirements of Directive 1999/5/EC.

The following standards were applied:

EMC	**EN 301 489-1(08-2002); EN 301 489-17(08-2002)**
	EN 55022:1994+A1: 1995+A2: 1997, Class B;
	EN 61000-3-2: 2000;EN 61000-3-3: 1995 + A1:2001
Radio	**EN 300 328 V1.6.1 (2004)**
Health & Safety	**EN 60950 (2000)**

The product carries the CE Mark:



Date & Place of Issue: May 5, 2005 – The Netherlands

Signature:

Ivar Beljaars
EMEA Product Manager & Systems Engineer
Haarlerbergpark Haarlerbergweg 13-19 1101 CH Amsterdam Netherlands

Additional Information:

EMC Test Report	*ADT Corp. Test Report Number: RM940322H02; May 05, 2005*
Radio Test Report	*ADT Corp. Test Report Number: RE940322H02; May 05, 2005*
Safety Test Report	*Cerpass Consultancy Corp. Test Report Number: 10001 122 001; April 01, 2005*





DECLARATION OF CONFORMITY

With regard to the R&TTE Directive 1999/5/EC

According to EN 45014

Cisco-Linksys LLC
121 Theory Drive
Irvine, CA 92617
USA

Declares under our sole responsibility that the product,

Linksys WAG354G / Wireless-G ADSL Home Gateway (Annex B)

Variants: WAG354G –XX where XX may stand for BG, BT, DE,FR, EU, E1, SE or UK (where applicable)

Fulfills the essential requirements of Directive 1999/5/EC.

The following standards were applied:

EMC	**EN 301 489-1(08-2002); EN 301 489-17(08-2002)**
	EN 55022:1994+A1: 1995+A2: 1997, Class B;
	EN 61000-3-2: 2000;EN 61000-3-3: 1995 + A1:2001
Radio	**EN 300 328 V1.6.1 (2004)**
Health & Safety	**EN 60950 (2000)**

The product carries the CE Mark:



Date & Place of Issue: May 5, 2005 – The Netherlands

Signature:

Ivar Beljaars
EMEA Product Manager & Systems Engineer
Haarlerbergpark Haarlerbergweg 13-19 1101 CH Amsterdam Netherlands

Additional Information:

EMC Test Report	*ADT Corp. Test Report Number: RM940322H02B; May 04, 2005*
Radio Test Report	*ADT Corp. Test Report Number: RE940322H02B; May 04, 2005*
Safety Test Report	*Cerpass Consultancy Corp. Test Report Number: 10001 131 001; April 29, 2005*